



ISO 27001:2022  
Lead Implementer

Programme de formation

# ISO 27001:2022

Lead Implementer

**Votre formation comprend deux parties essentielles à découvrir :**

## **Partie 1 :**

Grâce à notre partenariat avec PECB, vous disposez de 35h de vidéos exclusive PECB incluant des quiz pour valider les notions vues

## **Partie 2 :**

Parce qu'une approche normative n'est pas suffisante pour construire son SMSI, vous bénéficiez de plus de 20h supplémentaires de vidéos concernant l'implémentation de ce SMSI avec une vue opérationnelle.

# ISO 27001:2022

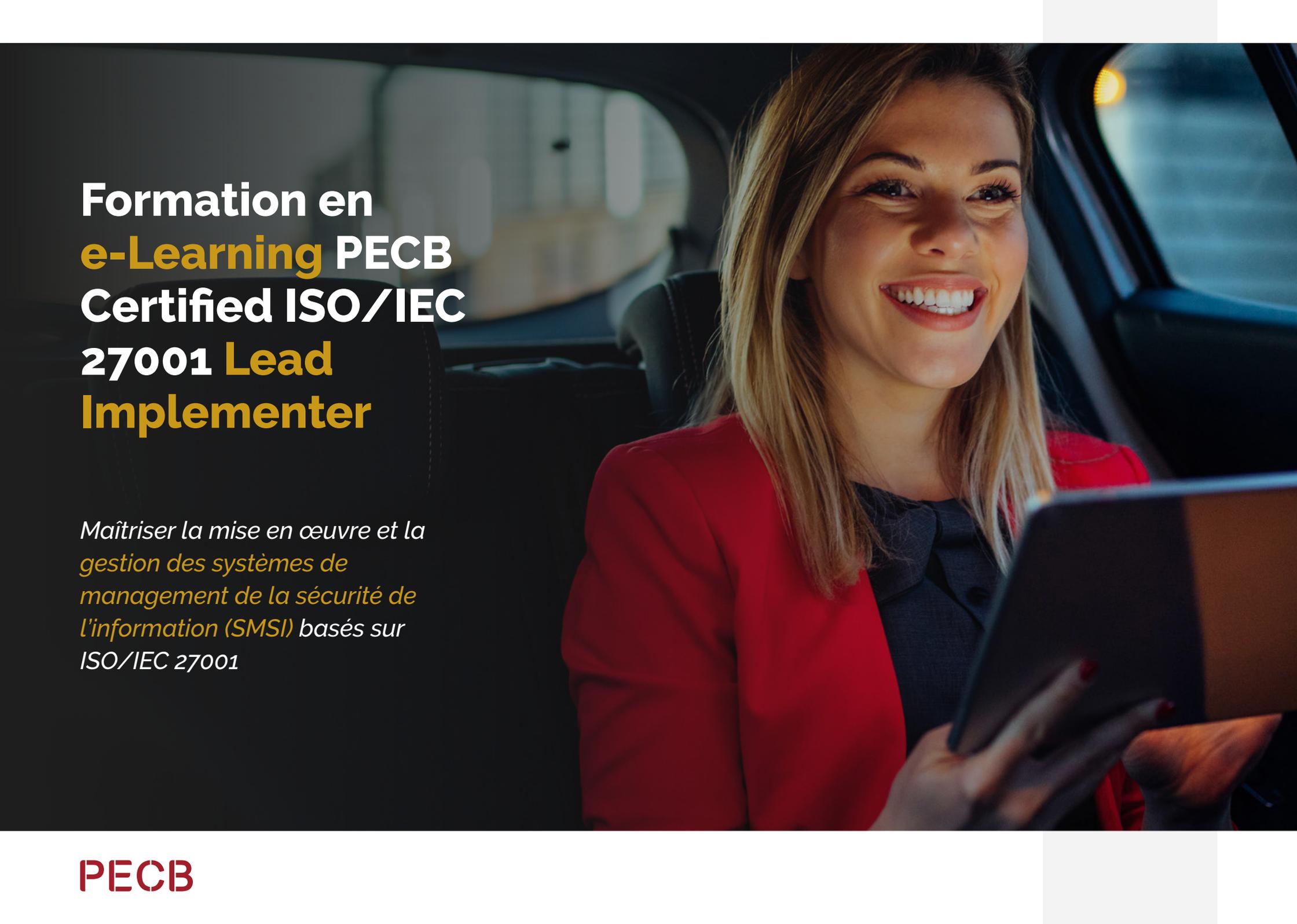
Lead Implementer

## Partie 1 :

Grâce à notre partenariat avec PECB, vous disposez de 35h de vidéos exclusive PECB incluant des quiz pour valider les notions vues.



# PECB

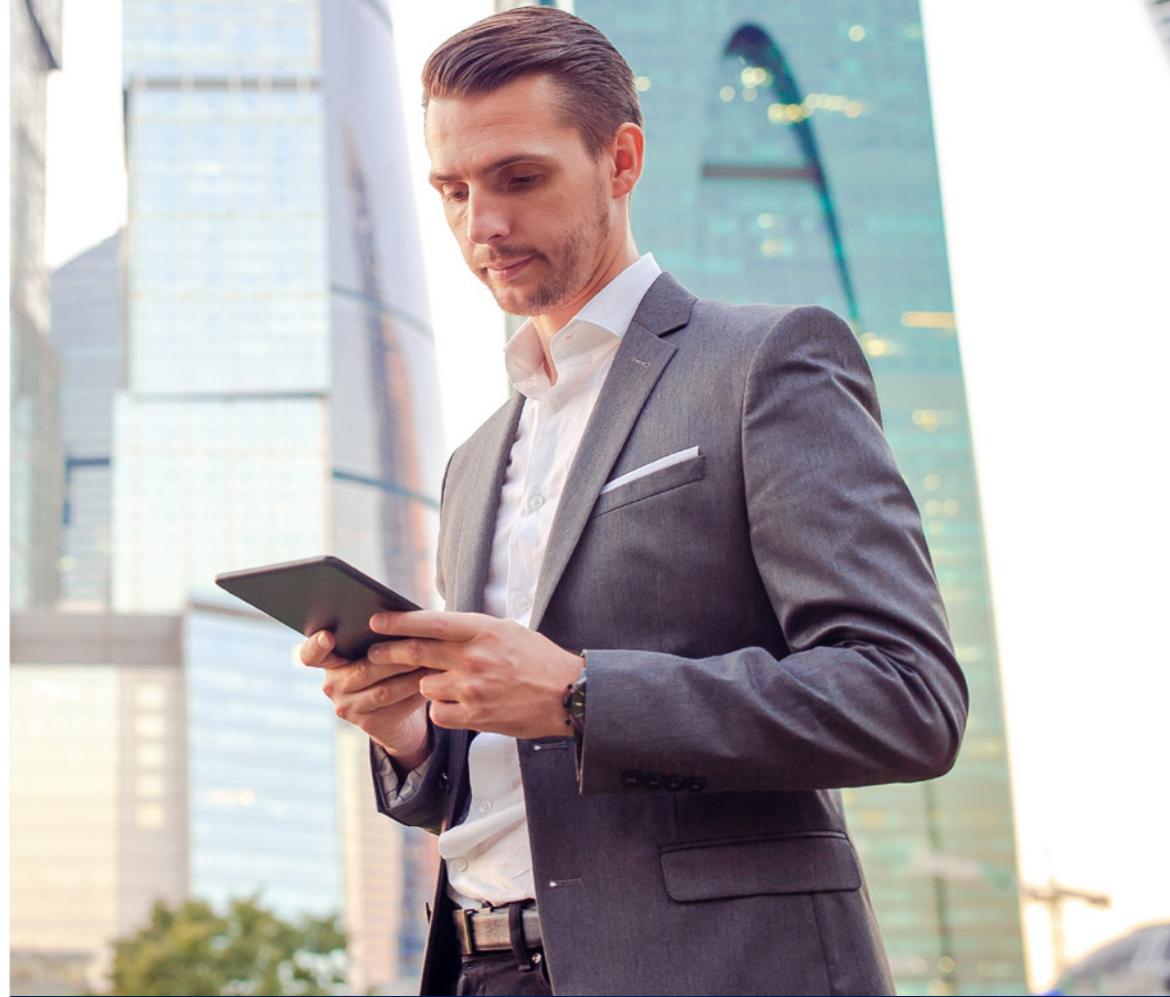


**Formation en  
e-Learning PECB  
Certified ISO/IEC  
27001 Lead  
Implementer**

*Maîtriser la mise en œuvre et la  
gestion des systèmes de  
management de la sécurité de  
l'information (SMSI) basés sur  
ISO/IEC 27001*

*Dans un monde qui bouge plus vite que jamais, les progrès technologiques ont rapidement évolué et redéfinissent, entre autres, notre façon de vivre, d'apprendre et d'enseigner. Le caractère expansif de l'Internet et de la technologie nous amène à trouver de nouvelles façons de nous adapter à ce nouvel environnement virtuel. Ce nouveau monde a donné naissance à une nouvelle forme d'étude, à la fois efficace et de portée mondiale : l'eLearning.*

*La formation en e-Learning ISO/IEC 27001 Lead Implementer est conçue pour vous aider à comprendre les approches pratiques liées à la mise en œuvre d'un système de management de la sécurité de l'information (SMSI) qui préserve la confidentialité, l'intégrité et la disponibilité des informations par la mise en œuvre d'un processus de management du risque.*





**EMMANUEL BESLÉAU**



**MICHÈLE COPITET**



**ROMAIN ROUSSEAU**

## ***Rencontrez les formateurs***

*Chaque formation en e-Learning est dispensée par plusieurs formateurs expérimentés du monde entier. Chaque formation est divisée en plusieurs sections et sous-sections vidéo. Les vidéos contiennent des animations qui appuient les propos du formateur. Ces animations correspondent aux sections fournies dans le mode traditionnel de formation. En vue de maintenir l'intérêt de nos participants, nous avons intégré des quiz dans nos formations en e-Learning.*

# À quoi ressemble l'expérience ISO/IEC 27001 Lead Implementer en e-Learning ?

Notre formation en e-Learning ISO/IEC 27001 Lead Implementer est dispensée sur l'application KATE. Une fois connecté à l'aide de votre compte PECB, vous pourrez parcourir les sections de la formation ISO/IEC 27001 Lead Implementer.

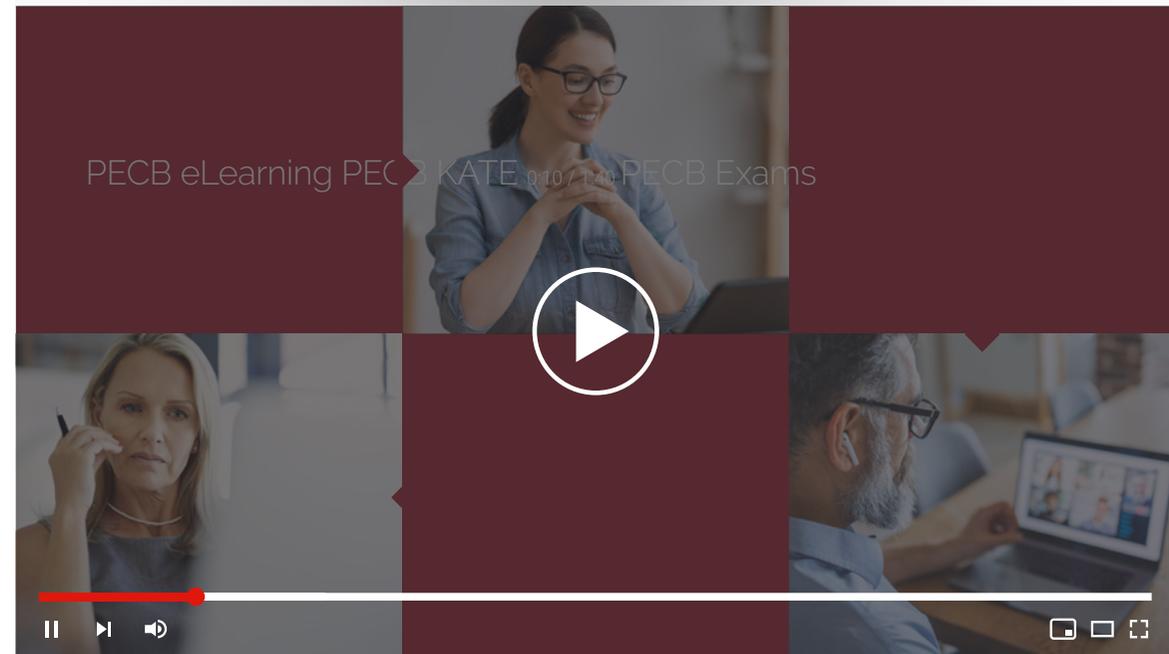
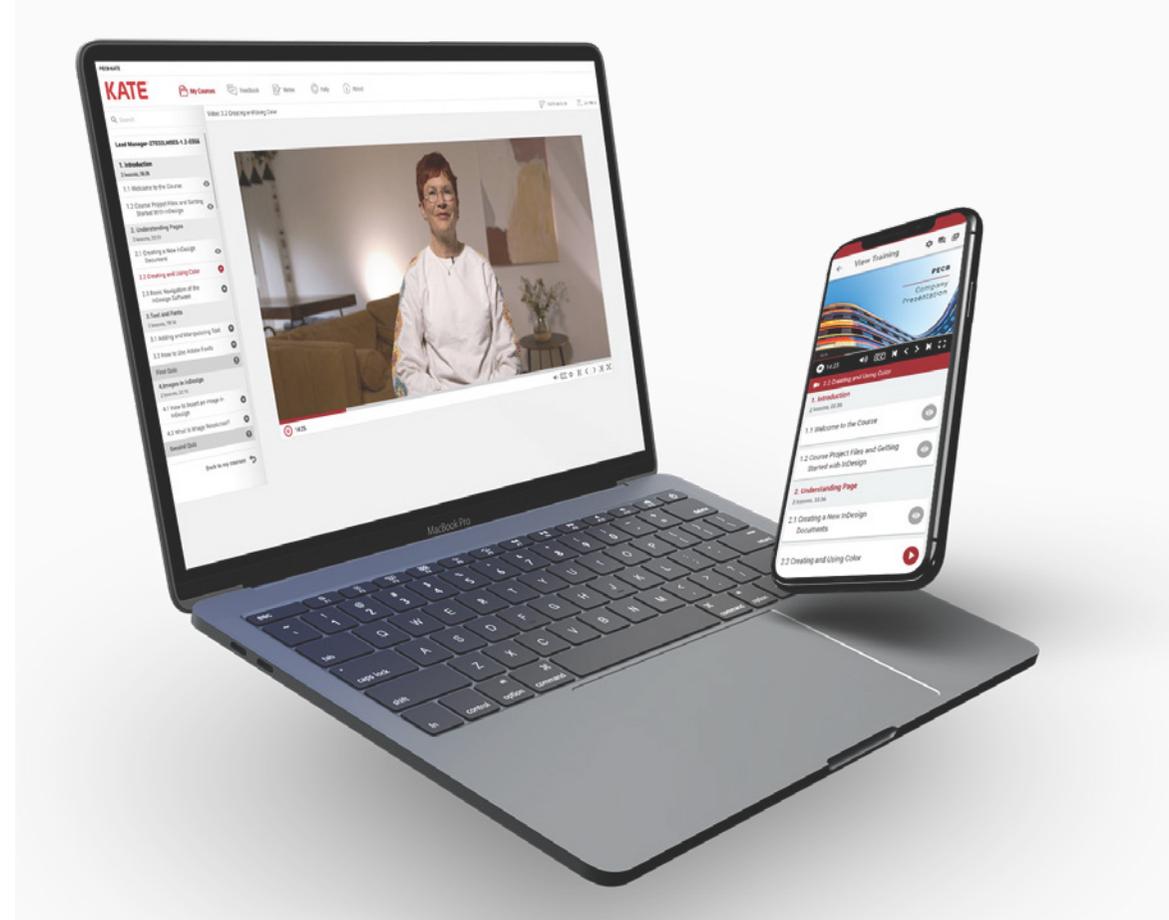
En plus de disposer du contenu de la formation au format vidéo, vous pourrez également accéder au format régulier des supports de formation structurés en différents jours de formation avec les fichiers supplémentaires disponibles dans un format modifiable (selon la formation, l'étude de cas, les exercices et les fichiers de clés de correction des exercices seront également disponibles).

En plus des cours magistraux et des supports de formation, des quiz ont été intégrés à l'application KATE afin de rendre nos formations aussi interactives que possible.

Suivre la formation

Accéder au matériel sur KATE

Passer l'examen à la date, à l'heure et au lieu qui vous conviennent le mieux via PECB Exams



## Comment pouvez-vous bénéficier de l'expérience e-Learning de PECB ?



Nos formations en e-Learning ont été conçues pour répondre aux besoins de divers apprenants qui ont des préférences d'apprentissage différentes ou un temps limité pour assister à une session de formation.

Voici quelques-uns des principaux avantages de l'expérience e-Learning de PECB :

*La totalité de la formation et de l'examen s'effectuant par voie électronique (d'où le « e » d'e-Learning), signifie que tout ce dont vous avez besoin pour accéder à ces formations est un appareil (par exemple, un ordinateur, une tablette, un téléphone intelligent), un accès Internet fonctionnel, et l'application KATE.*

*L'accès aux formations 24/7 vous permet de dicter le rythme à de votre apprentissage. Vous n'avez pas à vous soucier des horaires, des déplacements et de l'hébergement, ni de devoir prendre des jours de congé.*

*L'accès illimité vous permet de revenir à n'importe quelle section de la formation lorsque vous en avez besoin.*

*Chaque formation se compose de plusieurs sections vidéo. Cela a été fait dans le seul but de rendre l'information facile à recevoir et à traiter.*

*En résumé, les formations en e-Learning sont un moyen pratique d'améliorer efficacement vos compétences professionnelles. Votre classe virtuelle désormais, c'est KATE !*

# Pourquoi devriez-vous y participer?

Les menaces et les attaques contre la sécurité de l'information augmentent et s'améliorent constamment. La meilleure forme de défense contre ces menaces est la mise en œuvre et la gestion appropriées de mesures de sécurité et des bonnes pratiques. La sécurité de l'information constitue également une attente et une exigence essentielle des clients, des législateurs et des autres parties intéressées.

Cette formation en e-Learning est conçue pour vous préparer à la mise en œuvre d'un système de management de la sécurité de l'information (SMSI) basé sur les exigences de la norme ISO/IEC 27001. Elle vise à donner une compréhension complète des bonnes pratiques d'un SMSI et un cadre pour sa gestion et son amélioration continue.

Après avoir suivi cette formation en e-Learning, vous pouvez passer l'examen. Si vous le réussissez, vous pouvez demander le certificat « PECB Certified ISO/IEC

27001 Lead Implementer », qui démontre votre capacité et vos connaissances pratiques pour la mise en œuvre d'un SMSI basé sur les exigences d'ISO/IEC 27001.

# À qui s'adresse la formation ?

Chefs de projet et consultants impliqués et concernés par la mise en œuvre d'un SMSI

la mise en œuvre d'un SMSI  
Conseillers experts désireux de maîtriser

la conformité aux exigences de sécurité de  
Personnes chargées d'assurer  
l'information au sein d'un organisme.

Membres d'une équipe de mise en œuvre d'un SMSI



# Structure de la formation

## Section 1

Objectifs et structure de la formation

## Section 2

Normes et cadres réglementaires

## Section 3

Système de management de la sécurité de l'information (SMSI)

## Section 4

Concepts et principes fondamentaux de la sécurité de l'information

## Section 5

Initiation de la mise en œuvre du SMSI

## Section 6

Compréhension de l'organisation et de son contexte

## Section 7

Périmètre du SMSI

## Section 8

Leadership et approbation du projet

## Section 9

Structure organisationnelle

## Section 10

Analyse du système existant

## Section 11

Politique de sécurité de l'information

## Section 12

Gestion des risques

## Section 13

Déclaration d'applicabilité

## Section 14

Gestion des informations documentées

## Section 15

Sélection et conception des mesures

## Section 16

Mise en œuvre des mesures

## Section 17

Tendances et technologies

## Section 18

Communication

## Section 19

Compétence et sensibilisation

## Section 20

Gestion des opérations de sécurité

## Section 21

Suivi, évaluation, analyse et évaluation

## Section 22

Audit interne

## Section 23

Revue de direction

## Section 24

Traitement des non-conformités

## Section 25 Amélioration

continue

## Section 26

Préparation à l'audit de certification

## Section 27

Clôture de la formation

# Objectifs d'apprentissage

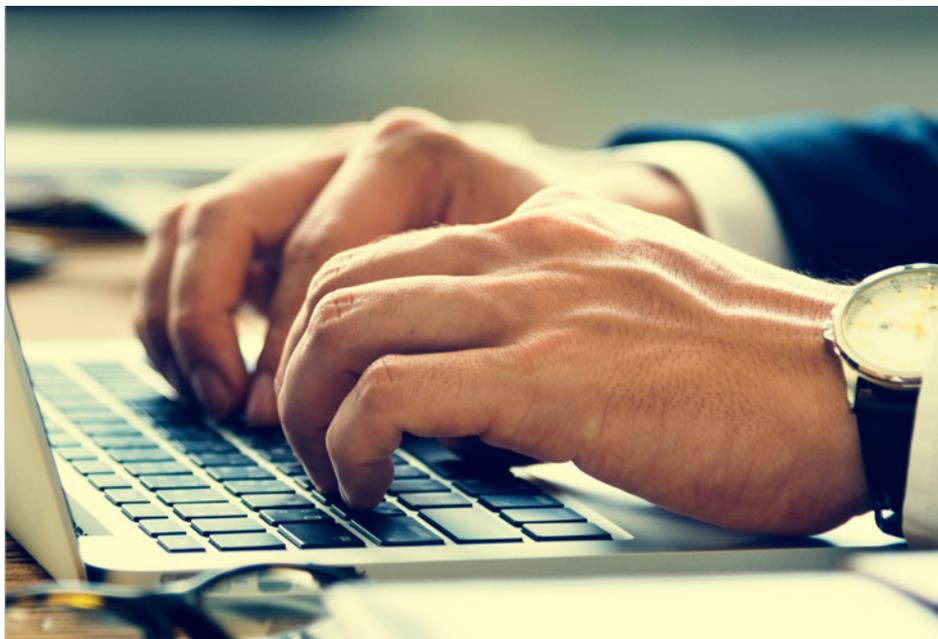
Acquérir une compréhension complète des concepts, approches, méthodes et techniques utilisés pour la mise en œuvre et la gestion efficace d'un SMSI

Comprendre la corrélation entre ISO/IEC 27001, ISO/IEC 27002 et d'autres normes et cadres réglementaires

Comprendre le fonctionnement d'un système de management de la sécurité de l'information et ses processus basés sur ISO/IEC 27001

Apprendre à interpréter et à mettre en œuvre les exigences à d'ISO/IEC 27001 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 SMSI



# Evaluation

L'examen « PECB Certified ISO/IEC 27001 Lead Implementer » répond pleinement aux exigences du Programme d'examen et de certification PECB (PEC). L'examen couvre les domaines de compétence suivants :

**Domaine 1 :** Principes et concepts fondamentaux d'un système de management de la sécurité de l'information (SMSI)

**Domaine 2 :** Système de management de la sécurité de l'information (SMSI)

**Domaine 3 :** Planification de la mise en œuvre d'un SMSI conforme à ISO/IEC 27001

**Domaine 4 :** Mise en œuvre d'un SMSI conforme à ISO/IEC 27001

**Domaine 5 :** Surveillance et mesure d'un SMSI conforme à ISO/IEC 27001

**Domaine 6 :** Amélioration continue d'un SMSI conforme à ISO/IEC 27001

**Domaine 7 :** Préparation à un audit de certification du SMSI

Pour des informations spécifiques sur le type d'examen, les langues disponibles et d'autres détails, veuillez consulter la liste des examens PECB et les Politiques et règlements relatifs à l'examen.

# Certification

Après avoir réussi l'examen, vous pouvez postuler pour l'une des certifications ci-dessous. Un certificat vous sera délivré si vous remplissez toutes les exigences relatives à la certification sélectionnée. Pour plus d'informations sur la certification ISO/IEC 27001 et le processus de certification de PECB, veuillez consulter les Politiques et règlements relatifs à la certification.

| Titre de compétence                                  | Examen   | Expérience professionnelle   | Expérience de projets SMSI | Autres exigences                      |
|--|--|--|----------------------------|---------------------------------------|
| PECB Certified ISO/IEC 27001 Provisional Implementer | Examen PECB Certified ISO/IEC 27001 Lead Implementer ou équivalent | Aucune   | Aucune                     | Signer le Code de déontologie de PECB |
| PECB Certified ISO/IEC 27001 Implementer             | Examen PECB Certified ISO/IEC 27001 Lead Implementer ou équivalent | Deux ans (dont un an en management de la sécurité de l'information)    | 200 heures                 | Signer le Code de déontologie de PECB |
| PECB Certified ISO/IEC 27001 Lead Implementer        | Examen PECB Certified ISO/IEC 27001 Lead Implementer ou équivalent | Cinq ans (dont deux ans en management de la sécurité de l'information) | 300 heures                 | Signer le Code de déontologie de PECB |
| PECB Certified ISO/IEC 27001 Senior Lead Implementer | Examen PECB Certified ISO/IEC 27001 Lead Implementer ou équivalent | Dix ans (dont sept ans en management de la sécurité de l'information)  | 1 000 heures               | Signer le Code de déontologie de PECB |

## Informations générales

Les frais de certification sont inclus dans le prix de l'examen.

Les participants recevront le support de cours contenant plus de 450 pages d'informations explicatives, d'exemples, de meilleures pratiques, d'exercices et de quiz.

Une Attestation d'achèvement de formation de 31 unités de FPC (Formation professionnelle continue) sera délivrée aux participants ayant assisté à la formation.

En cas d'échec à l'examen, les candidats peuvent le reprendre gratuitement dans les 12 mois suivant la première tentative.

**Remarque :** Les personnes certifiées PECB Lead Implementer et Lead Auditor sont qualifiées pour la certification PECB Master, pour autant qu'elles aient passé quatre examens Foundation supplémentaires liés à ce programme. Vous trouverez des informations plus détaillées sur les examens Foundation et les conditions d'obtention du titre Master [ici](#).

# ISO 27001:2022

Lead Implementer

## Partie 2 :

Une simple approche normative ne suffit pas pour établir votre SMSI.

Vous aurez accès à plus de 20 heures de vidéos supplémentaires sur la mise en œuvre de ce SMSI, enrichies par l'expérience d'e-Catalyst.



# ISO 27001:2022

Lead Implementer

## Votre formateur



En tant que Président de l'entreprise e-Catalyst, je suis un spécialiste en Gouvernance, Risques et Conformité (GRC) ainsi qu'en cybersécurité et j'exerce également comme auditeur senior pour les normes ISO 27001, 22301, entre autres.

Avec plus de 7 ans d'expérience dans le domaine de la cybersécurité et 5 ans en GRC, j'ai eu l'opportunité d'accompagner plus de 40 entreprises et de former plus de 500 individus sur des thématiques stratégiques en lien avec la sécurité de l'information et la conformité.

Je guide les entreprises dans la préparation à l'audit ISO 27001, l'élaboration de plans de continuité d'activité et la rédaction de la documentation d'un SMSI.



# ISO 27001:2022

## Lead Implementer

La seconde partie de notre formation en e-Learning est dispensée sur notre plateforme d'apprentissage.

Une fois connecté à l'aide de votre compte, vous pourrez parcourir les sections de la formation ISO/IEC 27001 Lead Implementer.

En plus de disposer du contenu de la formation au format vidéo, vous pourrez également accéder au format régulier des supports de formation structurés avec les fichiers supplémentaires disponibles dans un format modifiable.

En plus des cours magistraux et des supports de formation, des quiz ont été intégrés afin de rendre nos formations aussi interactives que possible.



# ISO 27001:2022

## Lead Implementer

### 1. Pilotage stratégique et engagement de la direction

- Acquisition et lecture de la norme ISO/IEC 27001:2022
- Compréhension de la vision et des objectifs de l'entreprise
- Élaboration et validation d'un business case
- Rédaction et approbation d'une charte de projet
- Désignation du responsable du SMSI
- Définition claire des rôles, responsabilités et autorités
- Mise en place du processus de gouvernance du SMSI
- Atelier pratique : Création des livrables

### 3. Analyse des écarts

- Définition de l'état cible de conformité
- Évaluation de l'état actuel de l'organisation
- Identification et formalisation des écarts
- Mise à jour du plan de projet en conséquence
- Atelier pratique : Création des livrables

### 2. Définition du périmètre du SMSI

- Analyse de contexte (enjeux internes et externes)
- Identification des parties intéressées et de leurs exigences
- Définition du périmètre (préliminaire, affiné, puis final)
- Validation du périmètre final par la direction
- Atelier pratique : Création des livrables

### 4. Politique de sécurité de l'information

- Mise en place des processus de gestion et de communication
- Définition des objectifs de sécurité
- Rédaction, validation et diffusion de la politique de sécurité
- Atelier pratique : Création des livrables

# ISO 27001:2022

Lead Implementer

## 5. Compétences et sensibilisation

- Identification des rôles clés
- Évaluation des besoins en formation et sensibilisation
- Mise en œuvre d'un programme adapté
- Évaluation de l'efficacité des actions menées
- Atelier pratique : Création des livrables

## 7. Méthodologie de gestion des risques

- Définition et validation des critères de risque
- Mise en place des processus d'appréciation et de traitement des risques
- Publication d'une politique de gestion des risques
- Atelier pratique : Création des livrables

## 6. Inventaire des actifs

- Politique de gestion des actifs et de classification de l'information
- Identification, cartographie, classification et étiquetage des actifs
- Désignation des propriétaires d'actifs
- Atelier pratique : Création des livrables

## 8. Appréciation des risques

- Identification des menaces, vulnérabilités, impacts, et responsables
- Analyse et évaluation des risques
- Documentation des résultats
- Atelier pratique : Création des livrables

# ISO 27001:2022

## Lead Implementer

### 9. Traitement des risques

- Élaboration et approbation du plan de traitement
- Détermination et mise en œuvre des mesures de sécurité
- Production et mise à jour de la Déclaration d'Applicabilité (Dd'A)
- Atelier pratique : Création des livrables

### 11. Évaluation des performances

- Mise en place d'indicateurs
- Mesure de l'efficacité et de la performance
- Réalisation des audits internes
- Organisation de la revue de direction
- Atelier pratique : Création des livrables

### 13. Audit de certification

- Sélection d'un organisme certificateur
- Planification et réalisation des audits de phase 1 et phase 2
- Atelier pratique : Création des livrables

### 10. Mise en œuvre et exploitation du SMSI

- Exploitation des processus du SMSI
- Contrôle des activités et des prestataires externalisés
- Atelier pratique : Création des livrables

### 12. Amélioration continue

- Détection des non-conformités
- Analyse des causes racines et actions correctives
- Suivi de l'efficacité des corrections apportées
- Atelier pratique : Création des livrables