Oo2 Formations
& Consulting

ISO 27001

ISO 27001 : ***Management de la Sécurité de l'Information***

PECB
AUTHORIZED
TITANIUM
PARTNER

+33 (0) 188 24 70 33 (+221) 33 825 45 54 / 33 825 72 34 +225 27 225 03 445 / 27 21 59 28 70 (+226) 55 77 87 11 / 55 79 11 42 (+229) 69 25 89 89

FAIRE CERTIFIER SON ORGANISATION ISO 27001

La certification ISO 27001 atteste que vous avez mis en place les mesures nécessaires pour assurer efficacement la sécurité de l'information, la cybersécurité et la protection des données à caractère personnel au sein de votre organisation. Par une approche de gestion du risque, vous démontrerez ainsi à vos parties intéressées que la sécurité de votre système d'information est pour vous un élément essentiel.

01 Vos objectifs principaux

- Améliorer la sécurité de votre système d'information et des données sensibles (financières, des clients, du personnel, etc.)
- Vous conformer aux règlementations de cybesécurité en vigueur, et ce, quel que soit le pays où vous exercez votre activité
- Anticiper en identifiant les menaces et les risques auxquels est confronté votre système d'information
- Rentabiliser votre investissement relatif à la sécurité de l'information en prenant un avantage concurrentiel
- Pérenniser votre activité en vous protégeant des cyberattaques, et éviter une perte financière ou un risque d'atteinte à l'image de votre organisation

02 Les étapes de la mise en œuvre

Etape 1 : Diagnostic et évaluation

- Établir un état des lieux de votre niveau de maturité et de conformité au regard de la norme
- Définir vos objectifs stratégiques et opérationnels
- Déterminer les risques et opportunités de votre activité et de vos opérations

Etape 2 : Déploiement

- Établir un plan d'actions pour vous mettre en conformité avec la norme
- Définir les indicateurs de performance
- Déployer le plan d'action en définissant le niveau de responsabilité des intervenants, en planifiant et en contrôlant la réalisation des actions
- Former les acteurs clés et sensibiliser l'ensemble des collaborateurs

Etape 3 : Contrôle, surveillance et amélioration

- Contrôler l'efficacité du SMSI
- Vous préparer à l'audit interne et à l'audit de certification
- Vous accompagner à mener la 1ère revue de direction
- Vous conseiller dans l'approche d'amélioration continue après analyse des non-conformités, du rapport d'audit et des changements identifiés

Etape 4 : Certification et renouvellement

- Nous faisons appel à notre partenaire PECB qui détachera un consultant indépendant pour venir auditer votre système et qui validera la certification
- Nous vous suivons pendant 3 ans pour vous assurer le renouvellement de votre certification

03 Les résultats

• Vous vous concentrez sur les éléments sensibles et saurez aborder le management de votre système par une approche en gestion du risque

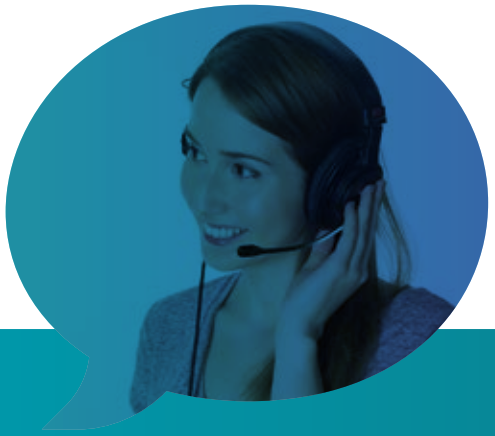
• Vous aurez une meilleure gestion de votre budget SI

• Vous mobiliserez l'ensemble de votre management et de votre personnel autour d'objectifs stratégiques et d'un perfectionnement de vos pratiques en continu

• Vous êtes reconnu internationalement dans la gestion de la sécurité de l'information et des données critiques

• Cet accompagnement vous permet d'obtenir votre certification plus rapidement et vous prépare à faire vivre votre système pour apporter les preuves nécessaires à votre démarche de management de votre système d'information

04 La gestion de votre SMSI



Pensez à l'externalisation

Afin d'assurer le renouvellement de la certification et éviter une précipitation chronophage et génératrice de stress, il est primordial de tenir à jour son SMSI et d'apporter les preuves d'une démarche d'amélioration continue.
Nous vous proposons de suivre vos équipes sécurité de l'information et/ou de réaliser des audits de surveillance. Ainsi vous vous garantissez l'efficacité et la pérennité de votre SMSI.

Nos équipes et modalités

Notre réseau d'experts présents en Europe et en Afrique allie expérience métier et expérience en consulting et audit. Nous saurons vous accompagner et vous assister dans la mise en œuvre d'un système de management de la sécurité de l'information et vous apporter l'objectivité nécessaire pour répondre aux défis que votre organisation doit relever, sans alourdir la bonne marche de votre activité.

Après un premier entretien pour évaluer le niveau de maturité de votre système d'information, nous définirons le nombre de jours d'intervention sur site et à distance.

Bon à savoir

La durée d'implémentation de la norme ISO 27001 jusqu'à l'audit de certification varie entre 9 et 14 mois. La certification est valable 3 ans. Nous vous en assurons le renouvellement par un suivi et un audit de surveillance annuel.

Demander un devis

Pour obtenir un devis rien de plus simple! Envoyez-nous un mail à consulting@oo2.fr. Nous vous retournerons un questionnaire à remplir qui nous permettra d'établir un devis au plus juste de votre projet de certification ISO 27001.

www.oo2.fr
consulting@oo2.fr
33 (0) 188 24 70 34

Les formations à la norme ISO 27001

ISO 27001 : Management de la sécurité de l'information – Foundation

2 jours code : ISO27001F

Objectifs

- Sensibilisation en matière de sécurité de l'information
- Réduction des failles de sécurité
- Avantage concurrentiel
- Démontrer une crédibilité et une confiance vis-à-vis des différents partenaires
- Conformité aux lois et aux règlements associés à la norme

Public

- Directeur de projet
- Responsable sécurité/RSSI

Prérequis

Implication dans la sécurité des systèmes d'information

Programme

- Introduction aux concepts du Système de Management de la Sécurité de l'Information (SMSI) tels que définis par la norme ISO 27001
- Mettre en œuvre des contrôles de la sécurité de l'information conformément à la norme ISO 27002

Examen de certification ISO 27001 Foundation : durée d'1 heure en Français

PECB AUTHORIZED TITANIUM PARTNER

Oo2 partenaire PECB

ISO 27001 : Management de la sécurité de l'information – Lead Implementer

4,5 jours code : ISO27001LI

Objectifs

- Comprendre la corrélation entre la norme ISO 27001 et la norme ISO 27002
- Maîtriser les concepts, méthodes et techniques pour mettre en oeuvre et gérer un SMSI
- Accompagner une organisation dans la mise en oeuvre, la gestion et la tenue à jour d'un SMSI

Public

- Responsable de la sécurité ou de la conformité de l'information au sein d'une organisation
- Membres de l'equipe de sécurité de l'information
- Consultant sécurité
- Expert technique de l'information
- Directeur de projets
- Responsable sécurité/RSSI

Prérequis

Avoir une expérience dans la sécurité des systèmes d'informations

Programme

Jour 1 : Introduction au concept de Système de Management de la Sécurité de l'Information (SMSI) tel que défini par la norme ISO/IEC 27001

- Introduction au système de management et à l'approche processus
- Présentation des normes ISO 27001, ISO 27002 et ISO 27003 et du cadre réglementaire
- Principes fondamentaux de la sécurité de l'information
- Analyse préliminaire et établissement du niveau de maturité d'un système de management de la Sécurité de l'Information existante basée sur la norme ISO 21827
- Rédaction de la rentabilité et de la planification de la mise en œuvre d'un SMSI

Jour 2 : Planification de la mise en œuvre d'un SMSI conforme à la norme ISO/IEC 27001

- Implémentation d'un SMSI et politiques de sécurité de l'information
- Sélection de l'approche et de la méthodologie d'évaluation des risques
- Gestion des risques : l'identification, l'analyse et le traitement des risques (en s'inspirant des orientations de la norme ISO 27005)
- Rédaction de la déclaration d'applicabilité (DdA)

Jour 3 : Mise en œuvre d'un SMSI conforme à la norme ISO/IEC 27001

- Mise en œuvre du cadre de gestion documentaire
- Conception des mesures et des procédures de rédaction
- Mise en œuvre des mesures
- Développement d'un programme de formation, de sensibilisation et de communication sur la sécurité de l'information
- Gestion des incidents (fondée sur les orientations de la norme ISO 27035)
- Gestion des opérations d'un SMSI

Jour 4 : Contrôler, surveiller, mesurer un SMSI et audit de certification du SMSI conformément à la norme ISO/IEC 27001

- Contrôle et suivi du SMSI
- Élaboration d'indicateurs de performance et des tableaux de bord en conformité avec la norme ISO 27004
- Audit interne du SMSI
- Examen de la gestion d'un SMSI
- Mise en œuvre d'un programme d'amélioration continue
- Préparation pour un audit de certification ISO 27001

Jour 5 : Examen de certification ISO 27001 Lead Implementer : durée de 3 heures en Français

ISO 27001 : Management de la sécurité de l'information – Lead Auditor

4,5 jours code : ISO27001LA

Objectifs

- Sensibilisation en matière de sécurité de l'information
- Réduction des failles de sécurité
- Avantage concurrentiel
- Démontrer une crédibilité et une confiance
- Conformité aux lois et aux règlements associés

Public

- Directeur des Systèmes d'Information (DSI)
- Responsable informatique
- Responsable sécurité/RSSI

Prérequis

Connaissances de la norme ISO 27001, ISO 27002 et de la norme ISO 19011

Programme

Jour 1 : Introduction aux concepts du Système de Management de la Sécurité de l'Information (SMSI) tels que définis par la norme ISO 27001

- Cadre normatif, réglementaire et juridique relatif à la sécurité de l'information
- Principes fondamentaux de la sécurité de l'information
- Processus de certification ISO 27001 Lead Auditor
- Système de Management de la Sécurité de l'Information (SMSI)
- Présentation détaillée des clauses 4 à 8 de la norme ISO 27001

Jour 2 : Planifier et initier un audit ISO 27001

- Concepts et principes fondamentaux de l'audit
- Approche de l'audit fondée sur des preuves
- Préparation d'un audit de certification ISO 27001
- Audit documentaire du SMSI
- Réalisation d'une séance d'ouverture

Jour 3 : Conduire un audit ISO 27001

- Communication lors de l'audit
- Procédures d'audit : l'observation, l'examen de documents, interviews et techniques d'échantillonnage
- Plans de test de vérification
- Formulation des conclusions de l'audit
- Élaboration des non-conformités

Jour 4 : Conclure et assurer le suivi d'un audit ISO 27001

- Documentation d'audit
- Examen de la qualité
- Mener une réunion de clôture d'un audit ISO 27001
- Évaluation des plans d'actions correctives
- Audit de surveillance
- Programme de gestion de l'audit interne

Jour 5 : Examen de certification ISO 27001 Lead Auditor : durée de 3 heures en Français