

CATALOGUE DE FORMATIONS

2024



Kedros Cybersécurité accompagne les entreprises et les administrations afin de protéger leur patrimoine informationnel avec une approche maîtrisée des risques. Notre apprentissage continu au travers de nos expériences clients et de nos travaux de veille nous permet d'apporter à nos stagiaires des formations de qualité avec de réels retours d'expérience.

Elever le niveau de jeu de la cybersécurité en France à travers la formation fait partie de nos convictions.

Grégoire Besluau, directeur général, formateur et associé.



formations@kedros-cybersecurite.fr



www.kedros-cybersecurite.fr

En cas de nécessité d'adaptation de l'accueil ou de la pédagogie (ex: situation de handicap), merci de vous rapprocher de ref-handi.form@kedros-cybersecurite.fr.

Nos formations sont dispensées en présentiel et/ou en visioconférence, au format inter ou intra entreprise.



 RÉPUBLIQUE FRANÇAISE

La [certification](#) qualité a été délivrée par **AFNOR Certification** au titre de la catégorie d'action suivante :

ACTIONS DE FORMATION

L'activité de formation de Kedros Cybersécurité est enregistrée sous le numéro 11756784475 auprès du préfet de région d'Ile-de-France

Découvrez toutes nos formations pour l'exercice 2023-2024

Formations *Lead* – Certifiantes

ISO 27001 Lead Implementer (LI) – Certifiante.....	4
ISO 27001 Lead Auditor (LA) – Certifiante	5
ISO 22301 Lead Implementer (LI) – Certifiante.....	6
ISO 22301 Lead Auditor (LA) – Certifiante	7

Formations *Risk* – Certifiantes

ISO 27005 Risk Manager (RM) – Certifiante	9
ISO 31000 Risk Manager (RM) – Certifiante	10

Formations *Foundation* – Certifiantes

ISO 27001 Foundation – Certifiante.....	12
ISO 27005 Foundation – Certifiante.....	13
ISO 22301 Foundation – Certifiante.....	14
ISO 31000 Foundation – Certifiante.....	15

Formations *Introduction*

ISO 27001 Introduction	17
ISO 31000 Introduction	18
ISO 27005 Introduction.....	18
ISO 22301 Introduction	19

Formations *RSSI & sur mesure*

Formation RSSI	21
Formation RSSI étendue.....	22
Formation sur mesure.....	23

Informations utiles

Modalités d'accès et d'évaluation & CGV.....	24
--	----

Formations Lead

ISO 27001 Lead Implementer

ISO 27001 Lead Auditor

ISO 22301 Lead Implementer

ISO 22301 Lead Auditor



ISO 27001 Lead Implementer (LI) – Certifiante

Objectifs

- Acquérir une compréhension globale 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 ainsi qu'avec 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 de la norme ISO 27001 dans le contexte spécifique d'un organisme
- Acquérir les connaissances nécessaires pour soutenir une organisation dans la planification, la mise en œuvre, la gestion, la surveillance et le maintien efficaces d'un SMSI

Public visé

- Chefs de projet et consultants impliqués et concernés par la mise en œuvre d'un SMSI
- Conseillers experts cherchant à maîtriser la mise en œuvre d'un SMSI
- Personnes responsables d'assurer la conformité aux exigences de sécurité de l'information au sein d'une organisation
- Membres d'une équipe de mise en œuvre d'un SMSI

Prérequis

La principale condition pour participer à cette formation est d'avoir une connaissance générale – même faible - des concepts du SMSI et d'ISO/IEC 27001

<u>Durée</u>	<u>Coût</u>
5 jours	3 500 € HT

Programme

- Jour 1 : Introduction à la norme ISO/IEC 27001 et initiation d'un SMSI
- Jour 2 : Planification de la mise en œuvre d'un SMSI
- Jour 3 : Mise en œuvre du SMSI
- Jour 4 : Suivi, amélioration continue et préparation à l'audit de certification du SMSI
- Jours 5 : Révisions par Kedros Cybersécurité et examen de certification

Après avoir maîtrisé l'ensemble des concepts relatifs aux Systèmes de management de la sécurité de l'information, vous pouvez vous présenter à l'examen et postuler au titre de « PECB Certified ISO/CEI 27001 Lead Implementer ».

En étant titulaire d'une certification PECB, vous démontrerez que vous disposez des connaissances pratiques et des compétences professionnelles pour mettre en œuvre la norme ISO/CEI 27001 dans une organisation.

Approche pédagogique

- Cette formation contient des exercices de type dissertation, des quiz à choix multiple, des exemples et les bonnes pratiques utilisées dans la mise en œuvre d'un SMSI
- Les participants sont encouragés à communiquer entre eux et à participer à des discussions lorsqu'ils complètent les quiz et les exercices
- Les exercices sont basés sur une étude de cas
- La structure des quiz est similaire à celle de l'examen de certification
- Kedros Cybersécurité propose son propre quiz d'entraînement à l'examen

Certification émise par PECB en cas de succès à l'examen

PECB

ISO 27001 Lead Auditor (LA) – Certifiante

Objectifs

- Expliquer les concepts et les principes fondamentaux d'un système de management de la sécurité de l'information (SMSI) basé sur ISO 27001
- Interpréter les exigences d'ISO 27001 pour un SMSI du point de vue d'un auditeur
- Évaluer la conformité du SMSI aux exigences d'ISO 27001, en accord avec les concepts et les principes fondamentaux d'audit
- Planifier, réaliser et clôturer un audit de conformité à ISO 27001, conformément aux exigences d'ISO/IEC 17021-1, aux lignes directrices d'ISO 19011 et aux autres bonnes pratiques d'audit
- Gérer un programme d'audit ISO/IEC 27001

Public visé

- Auditeurs souhaitant effectuer et diriger des audits de certification du système de management de sécurité de l'information (SMSI)
- Managers ou consultants souhaitant maîtriser le processus d'audit d'un système de management de sécurité de l'information
- Personnes responsables de maintenir la conformité aux exigences du système de management de sécurité de l'information.
- Experts techniques souhaitant se préparer à un audit du système de management de sécurité de l'information.
- Conseillers experts en management de sécurité de l'information

Prérequis

Une bonne connaissance de la norme ISO/CEI 27001 et des connaissances approfondies sur les principes de l'audit. Kedros Cybersécurité recommande de suivre au préalable la formation ISO 27001 Certified Lead Implementer. Contactez-nous en cas de doutes.

<u>Durée</u>	<u>Coût</u>
5 jours	3 500 € HT

Programme

- Jour 1 : Introduction au système de management de la sécurité de l'information (SMSI) et à ISO/IEC 27001
- Jour 2 : Principes d'audit, préparation et initiation d'un audit
- Jour 3 : Activités d'audit sur site
- Jour 4 : Clôture de l'audit
- Jours 5 : Révisions par Kedros Cybersécurité et examen de certification

Après avoir maîtrisé les concepts d'audit démontrés et réussi l'examen, vous pourrez demander la certification « PECB Certified ISO/IEC 27001 Lead Auditor ». Cette certification, reconnue à l'échelle internationale, démontre que vous possédez l'expertise et les compétences nécessaires pour auditer des organismes basés sur les bonnes pratiques.

Approche pédagogique

- Cette formation est basée à la fois sur la théorie et sur les meilleures pratiques utilisées dans l'audit du SMSI
- Les cours magistraux sont illustrés par des exemples basés sur une étude de cas
- Les exercices pratiques sont basés sur une étude de cas qui inclut des jeux de rôle et des discussions
- Les tests pratiques sont similaires à l'examen de certification
- Kedros Cybersécurité propose son propre quiz d'entraînement à l'examen

Certification émise par PECB en cas de succès à l'examen

PECB

ISO 22301 Lead Implementer (LI) – Certifiante

Objectifs

- Expliquer les concepts et principes fondamentaux d'un système de management de la continuité d'activité (SMCA) basé sur ISO 22301
- Interpréter les exigences d'ISO 22301 pour un SMCA du point de vue d'un responsable de la mise en œuvre
- Initier et planifier la mise en œuvre d'un SMCA basé sur ISO 22301, en utilisant la méthodologie IMS2 de PECB et d'autres bonnes pratiques
- Soutenir un organisme dans le fonctionnement, le maintien et l'amélioration continue d'un SMCA basé sur ISO 22301
- Préparer un organisme à un audit de certification par une tierce partie

Public visé

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

Prérequis

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

<u>Durée</u>	<u>Coût</u>
5 jours	3 500 € HT

Programme

- Jour 1 : Introduction à la norme ISO 22301 et initialisation d'un SMCA
- Jour 2 : Planification de la mise en œuvre d'un SMCA ;
- Jour 3 : Mise en œuvre d'un SMCA
- Jour 4 : Surveillance, mesure, amélioration continue et préparation de l'audit de certification du SMCA
- Jours 5 : Révisions par Kedros Cybersécurité et examen de certification

Après avoir maîtrisé les concepts d'audit démontrés et réussi l'examen, vous pourrez demander la certification « PECB Certified ISO/IEC 22301 Lead Implementer ». 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.

Approche pédagogique

- Cette formation est basée à la fois sur la théorie et sur les meilleures pratiques utilisées pour la mise en œuvre du SMCA
- Les cours magistraux sont illustrés par des exemples basés sur une étude de cas
- Les exercices pratiques sont basés sur une étude de cas qui inclut des jeux de rôle et des présentations orales
- Les tests pratiques sont similaires à l'examen de certification
- Kedros Cybersécurité propose son propre quiz d'entraînement à l'examen

Certification émise par PECB en cas de succès à l'examen

PECB

ISO 22301 Lead Auditor (LA) – Certifiante

Objectifs

- Expliquer les concepts et principes fondamentaux d'un système de management de la continuité d'activité (SMCA) basé sur ISO 22301
- Interpréter les exigences d'ISO 22301 pour un SMCA du point de vue d'un auditeur
- Évaluer la conformité du SMCA aux exigences d'ISO 22301, en accord avec les concepts et principes fondamentaux d'audit
- Planifier, conduire et clore un audit de conformité à ISO 22301, conformément aux exigences d'ISO/IEC 17021-1, aux lignes directrices d'ISO 19011 et aux autres bonnes pratiques d'audit
- Gérer un programme d'audit ISO 22301

Public visé

- 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
- Conseillers spécialisés en management de la continuité d'activité

Prérequis

Une bonne connaissance de la norme ISO 22301 et des connaissances approfondies sur les principes de l'audit

<u>Durée</u>	<u>Coût</u>
5 jours	3 500 € HT

Programme

- Jour 1 : Introduction au système de management de la continuité d'activité et à la norme ISO 22301
- Jour 2 : Principes, préparation et déclenchement de l'audit
- Jour 3 : Activités d'audit sur site
- Jour 4 : Clôture de l'audit
- Jours 5 : Révisions par Kedros Cybersécurité et examen de certification

Après avoir maîtrisé les concepts d'audit démontrés et réussi l'examen, vous pourrez demander la certification « PECB Certified ISO/IEC 22301 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.

Approche pédagogique

- Cette formation est basée à la fois sur la théorie et sur les meilleures pratiques utilisées dans l'audit du SMCA
- Les cours magistraux sont illustrés par des exemples basés sur une étude de cas
- Les exercices pratiques sont basés sur une étude de cas qui inclut des jeux de rôle et des présentations orales
- Les tests pratiques sont similaires à l'examen de certification
- Kedros Cybersécurité propose son propre quiz d'entraînement à l'examen

Certification émise par PECB en cas de succès à l'examen

PECB

Formations Risk Manager

ISO 27005 Risk Manager

ISO 31000 Risk Manager



ISO 27005 Risk Manager (RM) – Certifiante

Objectifs

- 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

Public visé

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

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

<u>Durée</u>	<u>Coût</u>
3 jours	2 200 € HT

Programme

- Jour 1 : Introduction au programme de gestion des risques conforme à ISO/IEI 27005
- Jour 2 : Mise en œuvre d'un processus de gestion des risques conforme à ISO/IEC 27005
- Jour 3 : Aperçu des autres méthodes d'appréciation des risques liés à la sécurité de l'information et examen de certification

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.

Approche pédagogique

- Cette formation est basée à la fois sur la théorie et sur les bonnes pratiques utilisées dans le management du risque de la sécurité de l'information
- Les sessions de cours sont illustrées par des exemples basés sur des études de cas
- Les exercices pratiques sont basés sur une étude de cas qui comprend des jeux de rôle et des discussions
- Les tests de pratique sont similaires à l'examen de certification
- Kedros Cybersécurité propose son propre quiz d'entraînement à l'examen

Certification émise par PECB en cas de succès à l'examen

PECB

ISO 31000 Risk Manager (RM) – Certifiante

Objectifs

- Comprendre les principes de management du risque, tels que formulés dans ISO 31000
- Établir, maintenir et améliorer continuellement un cadre de management du risque, conformément aux lignes directrices d'ISO 31000
- Appliquer le processus de management du risque, conformément aux lignes directrices d'ISO 31000

Public visé

- Gestionnaires ou consultants chargés du management efficace du risque dans un organisme
- Toute personne désirant acquérir des connaissances approfondies sur les concepts, processus et principes de management du risque
- Conseillers impliqués dans le management du risque

Prérequis

Une compréhension fondamentale de la norme ISO/IEC 31000 et une connaissance approfondie de l'évaluation des risques et de la sécurité de l'information

<u>Durée</u>	<u>Coût</u>
3 jours	2 200 € HT

Programme

- Jour 1 : Introduction au programme de gestion des risques conforme à ISO/IEC 31000 ;
- Jour 2 : Mise en œuvre d'un processus de gestion des risques conforme à ISO/IEC 31000 ;
- Jour 3 : Techniques d'appréciation du risque conformes à la norme ISO 31010 et examen de certification ;

Après avoir appréhendé les concepts relatifs au management du risque, vous pouvez vous présenter à l'examen et postuler au titre de « PECB Certified ISO 31000 Risk Manager ». En étant titulaire d'une certification PECB, vous démontrerez que vous disposez des connaissances et des compétences pratiques pour gérer efficacement un processus du risque dans un organisme. Cette formation est conçue de manière à vous doter d'une maîtrise des meilleures pratiques en matière de management du risque et à développer vos aptitudes pour les mettre en œuvre dans un organisme afin de mettre en œuvre efficacement un processus de management du risque.

Approche pédagogique

- Cette formation est basée à la fois sur la théorie et sur les meilleures pratiques utilisées dans le management du risque
- Les cours magistraux sont illustrés par des exemples basés sur une étude de cas
- Les exercices pratiques sont basés sur une étude de cas qui inclut des jeux de rôle et des présentations orales
- Les tests pratiques sont similaires à l'examen de certification
- Kedros Cybersécurité propose son propre quiz d'entraînement à l'examen

Certification émise par PECB en cas de succès à l'examen

PECB

Formations Foundation

ISO 27001 Foundation

ISO 27005 Foundation

ISO 22301 Foundation

ISO 31000 Foundation

Les formations « Foundation » permettent d'appréhender les éléments fondamentaux des normes concernées.

D'une durée de 2 jours, elles sont idéales pour renforcer des connaissances, valider des notions et le vocabulaire clé des référentiels.

Elles sont également certifiantes !



ISO 27001 Foundation – Certifiante

Objectifs

- 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 27001:2022 et ISO/IEC 27002 ainsi qu'avec d'autres normes et cadres réglementaires
- 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

Public visé

- Toute personne impliquée dans le management de la sécurité de l'information
- Personnes souhaitant acquérir des connaissances relatives aux principaux processus du Système de management de la sécurité de l'information
- Personnes souhaitant poursuivre une carrière dans le management de la sécurité de l'information

Prérequis

Aucun prérequis n'est nécessaire pour participer à cette formation

<u>Durée</u>	<u>Coût</u>
2 jours	1 250 € HT

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 27001:2022
- Jour 2 : Exigences relatives au Système de management de la sécurité de l'information et examen de certification

La formation ISO/IEC 27001:2022 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/IEC 27001:2022. 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 27001:2022 Foundation ». La certification PECB Foundation atteste que vous avez compris les méthodes fondamentales, les exigences, le cadre et l'approche de management.

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
- Kedros Cybersécurité propose son propre quiz d'entraînement à l'examen

Certification émise par PECB en cas de succès à l'examen

PECB

ISO 27005 Foundation – Certifiante

Objectifs

- Décrire les principaux concepts, principes et définitions de la gestion des risques
- Interpréter les lignes directrices de la norme ISO/IEC 27005 pour la gestion des risques liés à la sécurité de l'information
- Identifier les approches, les méthodes et les techniques utilisées pour la mise en œuvre et la gestion d'un programme de gestion des risques liés à la sécurité de l'information

Public visé

- Professionnels de la gestion des risques
- Professionnels souhaitant se familiariser avec les lignes directrices de la norme ISO/IEC 27005 pour la gestion des risques liés à la sécurité de l'information
- Personnel chargé de la gestion des risques liés à la sécurité de l'information dans son domaine de responsabilité
- Personnes intéressées par une carrière dans la gestion des risques liés à la sécurité de l'information

Prérequis

Aucun prérequis n'est nécessaire pour participer à cette formation

<u>Durée</u>	<u>Coût</u>
2 jours	1 250 € HT

Programme

- Jour 1 : Introduction à la norme ISO/IEC 27005 et aux concepts fondamentaux de la gestion des risques liés à la sécurité de l'information
- Jour 2 : Gestion des risques liés à la sécurité de l'information et examen

ISO/IEC 27005 Foundation est une formation de deux jours consacrée au processus de gestion des risques liés à la sécurité de l'information introduit par ISO/IEC 27005 et à la structure de la norme. Elle donne une vue d'ensemble des lignes directrices de la norme ISO/IEC 27005 pour la gestion des risques liés à la sécurité de l'information, y compris l'établissement du contexte, l'évaluation du risque, le traitement du risque, la communication et concertation, l'enregistrement et le rapport, ainsi que la surveillance et revue.

Au terme de cette formation, vous pourrez vous présenter à l'examen. Si vous réussissez l'examen, vous pourrez postuler pour la certification PECB ISO 27005 Foundation. Cette certification est la preuve que vous avez une connaissance générale des lignes directrices de la norme ISO/IEC 27005 pour la gestion des risques liés à la sécurité de l'information.

Approche pédagogique

- Comprend des leçons illustrées par des exemples et des discussions
- Encourage l'interaction entre les participants à travers des questions et des suggestions
- Inclut des quiz dont la structure est similaire à celle de l'examen
- Kedros Cybersécurité propose son propre quiz d'entraînement à l'examen

Certification émise par PECB en cas de succès à l'examen

PECB

ISO 22301 Foundation – Certifiante

Objectifs

- Décrire les concepts, principes et définitions du management de la continuité d'activité
- Expliquer les principales exigences d'ISO 22301 pour un système de management de la continuité d'activité (SMCA)
- Identifier les approches et les techniques utilisées pour la mise en œuvre et la gestion d'un SMCA

Public visé

- Toute personne impliquée dans le management de la continuité d'activité
- Personnes souhaitant acquérir des connaissances relatives aux principaux processus d'un Système de management de la continuité d'activité
- Personnes souhaitant poursuivre une carrière dans le management de la continuité d'activité

Prérequis

Aucun prérequis n'est nécessaire pour participer à cette formation

<u>Durée</u>	<u>Coût</u>
2 jours	1 250 € HT

Programme

- Jour 1 : Introduction au Système de management de la continuité d'activité (SMCA) et à la norme ISO 22301
- Jour 2 : Système de management de la continuité d'activité et examen de certification

La présente formation a été élaborée 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 suivant 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, l'audit interne, la revue de direction et le processus d'amélioration continue.

À l'issue de la formation, vous pourrez vous présenter à l'examen et, si vous le réussissez, vous pourrez demander le titre de « PECB Certificate Holder in ISO 22301 Foundation ». Un certificat PECB Foundation est la preuve que vous disposez de connaissances sur les concepts fondamentaux, les principes, les méthodologies, les exigences, le cadre et l'approche de gestion utilisés dans 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
- Kedros Cybersécurité propose son propre quiz d'entraînement à l'examen

Certification émise par PECB en cas de succès à l'examen

PECB

ISO 31000 Foundation – Certifiante

Objectifs

- Résumer les principaux concepts et principes du management du risque tels qu'ils sont définis dans la norme ISO 31000
- Expliquer les lignes directrices d'ISO 31000 pour l'établissement du cadre de management du risque
- Décrire l'application du processus de management du risque conformément aux lignes directrices d'ISO 31000

Public visé

- Professionnels du management du risque
- Les personnes souhaitant acquérir des connaissances sur les lignes directrices ISO 31000 relatives aux principes, au cadre et au processus de management du risque
- Personnes responsables de la création et de la protection de la valeur au sein d'une organisation
- Personnel chargé du management du risque et des opportunités dans son domaine de responsabilité
- Les personnes intéressées par une carrière de manager du risque

Prérequis

Aucun prérequis n'est nécessaire pour participer à cette formation

Durée	Coût
2 jours	1 250 € HT

Programme

- Jour 1 : Introduction à la gestion des risques, aux composantes de la norme ISO 31000 et initiation au processus de gestion des risques
- Jour 2 : L'évaluation des risques, le traitement du risque, enregistrement et élaboration de rapports, suivi et revue, communication et consultation selon la norme ISO 31000

La formation ISO 31000 Foundation présente les principes de base et les approches de la gestion des risques et des opportunités sur la base des lignes directrices de la norme ISO 31000. Cette formation se concentre sur les éléments fondamentaux de la norme ISO 31000 : termes fondamentaux et définitions, les principes de la gestion des risques, le cadre de la gestion des risques et le processus de gestion des risques. En outre, chaque étape du processus de gestion des risques est analysée et détaillée individuellement.

Au terme de la formation, vous pouvez vous présenter à l'examen et postuler pour la certification PECB ISO 31000 Foundation. Cette certification est la preuve que vous avez compris les concepts fondamentaux du risque et les méthodologies de gestion des risques basées sur les lignes directrices de la norme ISO 31000.

Approche pédagogique

- Cette formation est basée à la fois sur la théorie et sur les meilleures pratiques utilisées dans le management du risque
- Les cours magistraux sont illustrés par des exemples basés sur une étude de cas
- Les exercices pratiques sont basés sur une étude de cas qui inclut des jeux de rôle et des présentations orales
- Les tests pratiques sont similaires à l'examen de certification
- Kedros Cybersécurité propose son propre quiz d'entraînement à l'examen

Certification émise par PECB en cas de succès à l'examen

PECB

Formations Introduction

ISO 27001 Introduction

ISO 27005 Introduction

ISO 31000 Introduction

ISO 22301 Introduction

Les formations « Introduction » permettent de découvrir les référentiels concernés.

Introduction de notions, découverte du vocabulaire clé, parfait pour sensibiliser vos collaborateurs et collaboratrices gravitant autour des projets concernés.



ISO 27001 Introduction

Objectifs

- 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

Public visé

- Les personnes intéressées par le management de la sécurité de l'information
- Les personnes souhaitant acquérir des connaissances relatives aux principaux processus du Système de management de la sécurité de l'information

Prérequis

Aucun prérequis n'est nécessaire pour participer à cette formation

<u>Durée</u>	<u>Coût</u>
1 jour	600 € HT

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

La formation d'introduction à la norme ISO/IEC 27001 vous permettra d'appréhender les concepts fondamentaux d'un Système de management de la sécurité de l'information.

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.

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

La formation d'introduction à la norme ISO/IEC 27001 vous permettra d'appréhender les concepts fondamentaux d'un Système de management de la sécurité de l'information.

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.

ISO 27005 Introduction

Objectifs

- 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

Public visé

- Les personnes intéressées par la gestion des risques liés à la sécurité de l'information
- Les personnes souhaitant acquérir des connaissances relatives aux principaux processus de la gestion des risques liés à la sécurité de l'information

Prérequis

Aucun prérequis n'est nécessaire pour participer à cette formation

<u>Durée</u>	<u>Coût</u>
1 jour	600 € HT

Programme

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

La formation d'introduction à la norme ISO/IEC 27005 vous permettra d'appréhender les concepts fondamentaux relatifs à la gestion des risques liés à la sécurité de l'information en utilisant la norme ISO/IEC 27005 comme cadre de référence.

En participant à la formation d'introduction ISO/IEC 27005, vous allez comprendre l'importance de la gestion des risques liés à la sécurité de l'information et les avantages que peuvent en tirer les entreprises, la société et le gouvernement.

ISO 31000 Introduction

Objectifs

- Connaître les concepts, approches, méthodes et techniques permettant de gérer les risques
- Comprendre les processus fondamentaux du management du risque

Public visé

- Les personnes intéressées par le management du risque
- Les personnes souhaitant acquérir des connaissances relatives aux principaux processus du management du risque

Prérequis

Aucun prérequis n'est nécessaire pour participer à cette formation

<u>Durée</u>	<u>Coût</u>
1 jour	600 € HT

Programme

- Jour 1 : Introduction au management du risque selon les principes et les lignes directrices de la norme ISO 31000

La formation d'introduction à la norme ISO 31000 vous permettra d'appréhender les concepts fondamentaux du management du risque.

En participant à la formation d'introduction ISO 31000, vous allez comprendre l'importance du management du risque et les avantages que peuvent en tirer les entreprises, la société et le gouvernement.

ISO 22301 Introduction

Objectifs

- 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

Public visé

- Les personnes intéressées par le management de la continuité d'activité
- Les personnes souhaitant acquérir des connaissances relatives aux principaux processus du Système de management de la continuité d'activité

Prérequis

Aucun prérequis n'est nécessaire pour participer à cette formation

<u>Durée</u>	<u>Coût</u>
1 jour	600 € HT

Programme

- Introduction aux concepts du Système de management de la continuité d'activité, tels que définis par 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.

Formations RSSI

RSSI

RSSI étendue

Formation sur mesure

Formation RSSI

Objectifs

- Connaître les concepts, approches, méthodes et techniques permettant de gérer la sécurité du patrimoine informationnel d'une entreprise
- Comprendre la sécurité opérationnelle, la gestion du risque et mettre en œuvre des éléments de contrôle concrets

Public visé

- RSSI principalement, mais aussi :
- Analyste sécurité
- Correspondant(e) sécurité
- Chef(fe) de projet
- Juriste

Prérequis

Aucun prérequis n'est nécessaire pour participer à cette formation

<u>Durée</u>	<u>Coût</u>
2 jours	1300 € HT

Programme

- Introduction
- Gestion des risques
- PSSI
- Les métiers de l'entreprise
- Accueillir le collaborateur
- Intégration de la sécurité dans les projets (ISP)
- Sécurité opérationnelle & indicateurs sur :
 - Patch management
 - Couverture anti virale
 - Sécurité réseau
 - Gestion des socles
 - Gestion des sauvegardes
 - Développement sécurisé
- Défis de l'identité
- Gestion des tiers et PAS
- Panorama des standards et normes

Approche pédagogique

- Cette formation est basée à la fois sur la théorie et sur les meilleures pratiques utilisées les activités de gouvernance en cybersécurité
- Les cours magistraux et exercices sont basés sur des exemples concrets
- Les tests pratiques font l'objet de corrections collectives

Programme

- Introduction
- Gestion des risques
- PSSI
- Les métiers de l'entreprise
- Accueillir le collaborateur
- Intégration de la sécurité dans les projets (ISP)
- Sécurité opérationnelle & indicateurs sur :
 - Patch management
 - Couverture anti virale
 - Sécurité réseau
 - Gestion des socles

Formation RSSI étendue

Objectifs

- Connaître les concepts, approches, méthodes et techniques permettant de gérer la sécurité du patrimoine informationnel d'une entreprise
- Comprendre la sécurité opérationnelle, la gestion du risque et mettre en œuvre des éléments de contrôle concrets
- Enrichir ses connaissances sur des thématiques ciblées

Public visé

- RSSI principalement, mais aussi :
- Analyste sécurité
- Correspondant(e) sécurité
- Chef(fe) de projet
- Juriste

Prérequis

Aucun prérequis n'est nécessaire pour participer à cette formation

<u>Durée</u>	<u>Coût</u>
3 jours	1650 € HT

Programme

La formation « RSSI étendu » contient le programme de la formation RSSI et ajoute une 3^e journée de cours en détaillant parmi les points ci-dessous.

Cryptographie

- Chiffrement symétrique et asymétrique
- Signature, Protocoles cryptographiques
- Gestion des clés & Infrastructures (PKI)

Principes de sécurité des réseaux

- Cloisonnement réseau (filtrage, segmentation, micro-segmentation)
- Menaces réseaux (écoute passive, IP spoofing ...)
- Menaces protocolaires (flooding, DdoS ...)
- VPN – Virtual Private Network
- Protocoles de sécurité – IPsec / SSL
- NAC
- Authentification MFA

ISO 27001 & gestion des risques – approfondissements

- SMSI : définition et objectifs
- Vocabulaire clé
- Exigences de la norme
- Méthodologies d'appréciation et de traitement des risques
- Principes d'amélioration continue

Ou tout autre sujet jugé utile pour votre organisme !

La liste n'est pas exhaustive, aussi contactez-nous pour déterminer quelles thématiques ajouter afin d'obtenir une formation 100% sur mesure !

Formation sur mesure

Vous souhaitez vous mettre à jour sur des notions en cybersécurité sans pour autant resuivre un cycle complet de formation ? Vous voulez apprendre ou comprendre la cybersécurité organisationnelle avec un programme à la carte et sur mesure ?



Profitez de notre expertise et de notre savoir-faire : de la demi-journée de piqûre de rappel à la semaine complète d'approfondissement, nous sommes capables de vous proposer un programme pertinent et utile à votre fonction.

<u>Durée</u>	<u>Coût</u>
1-15 jours	Sur devis

Modalités et délais d'accès – modalités d'évaluation - CGV

Toutes nos formations sont assujetties à nos conditions générales de vente et disposent de modalités d'accès et d'évaluation décrites aux références suivantes :

Conditions générales de vente :



<https://kedros-cybersecurite.fr/cgv-formationen/>

Modalités d'inscription et d'évaluation :



<https://kedros-cybersecurite.fr/modalites-acces-et-evaluation/>



 RÉPUBLIQUE FRANÇAISE

La certification qualité a été délivrée par **AFNOR Certification** au titre de la catégorie d'action suivante :

ACTIONS DE FORMATION



Kedros
Cybersécurité

www.kedros-cybersecurite.fr