AUDIT – CONSEIL – FORMATION
EN CYBERSECURITE

POLARIS
SECURE TECHNOLOGIES

CATALOGUE FORMATIONS
Semestre 1 – 2021

FRANCE

37 RUE D'ALSACE 69800 ST-PRIEST

+33 4 78 74 50 80 / +33 7 86 00 47 79

SÉNÉGAL

LIBERTÉ 6 EXT BP 21207 DAKAR PONTY

+221 77 778 10 10 / +221 33 867 25 30

contact@polaris-st.com
www.polaris-st.com

POLARIS
SECURE TECHNOLOGIES

Qui sommes-nous ?

Fondé en 2010, Polaris Secure Technologies est un cabinet de conseil spécialisé dans la sécurité des systèmes d'information.
Fondé en 2010, Polaris Secure Technologies est un cabinet de conseil spécialisé dans la sécurité des systèmes d'information. Pure Player de la cybersécurité, Polaris ST vous accompagne dans la conception et la mise en œuvre de votre stratégie de cybersécurité. Elle accompagne également dans la mise en conformité ISO 27001, PCI DSS, RGPD, ... ou dans le choix de solutions techniques permettant de répondre à vos besoins, en toute indépendance par rapport aux constructeurs et éditeurs.
Son approche globale - à travers l'Audit, le Conseil et la Formation - a pour objectif de vous garantir une très bonne maitrise de la sécurité de votre système d'information.
Polaris ST a formé plus de deux mille (2.000) personnes ces dix dernières années, en Afrique et en Europe : DSI, RSSI, Consultants, Experts, Ingénieurs ou étudiants dans les écoles d'Ingénieurs et Universités. Il a accompagné plusieurs dizaines aux certifications.

Les trois leitmotivs de Polaris ST :

- L'AUDACE dans l'approche, dans l'innovation, dans le choix des solutions, dans l'ouverture à l'international, …
- LA SATISFACTION CLIENT par la qualité de nos prestations, par une écoute active, par la confidentialité
- LA PÉDAGOGIE ET LA SIMPLICITÉ par la facilité à rendre accessible les concepts techniques les plus complexes de la sécurité.

NOSSESSIONS

SESSIONS	DATE	LIEU	PRIX[1]
E-learning : 27001 LI et LA en français et en anglais	Selon votre disponibilité	E-learning	790 €
ISO 27001 Lead Implementer – Certification ISO (LSTI)	10 au 12 mars puis 22 au 23 mars	Classe Virtuelle	1 690 €
ISO 27001 Lead Auditor – Certification ISO (LSTI)	10 au 12 mars puis 15 au 16 mars	Classe Virtuelle	1 690 €
ISO 27005 Risk Manager – Certification ISO (PECB)	29 au 31 mars	Classe Virtuelle	1 290 €
ISO 27001 Lead Implementer – Certification ISO (PECB)	05 au 09 avril	Conakry	1 890 €
ISO 27001 Lead Implementer – Certification ISO (PECB)	03 au 07 mai	Brazzaville	1 890 €
ISO 27001 Lead Implementer – Certification ISO (PECB)	17 au 21 mai	Abidjan	1 890 €
ISO 27005 Risk Manager – Certification ISO (PECB)	31 mai au 02 juin	Paris	1 490 €
ISO 27001 Lead Implementer – Certification ISO (PECB)	07 au 11 juin	Libreville	1 890 €
ISO 27001 Lead Implementer – Certification ISO (PECB)	14 au 18 juin	Dakar	1 890 €
ISO 27001 Lead Auditor – Certification ISO (PECB)	28 juin au 02 juillet	Dakar	1 890 €
CISSP, Préparation à la Certification Sécurité (ISC)[2]	05 au 09 juillet	Dakar	2 290 €
CISSP, Préparation à la Certification Sécurité (ISC)[2]	19 au 23 juillet	Abidjan	2 290 €
ISO 27001 Lead Implementer – Certification ISO (PECB)	02 au 6 août	Mali	1 890 €
ISO 27001 Lead Implementer – Certification ISO (PECB)	17 au 21 août	Nouakchott	1 890 €
ISO 22301 Lead Auditor – Certification ISO (PECB)	06 au 10 sept.	Classe virtuelle	1 590 €
ISO 22301 Lead Implementer – Certification ISO (PECB)	20 au 24 sept.	Paris	1 790 €
ISO 27001 Lead Implementer – Certification ISO (PECB)	20 au 24 sept.	Niamey	1 890 €

Informations et inscription : +22177 778. 10 10 / +22133 867 25 30 / +33 4 78 74 50 80 / contact@polaris-st.com

[1] Prix hors taxe. Le cas échéant, frais d'examen compris.

CERTIFICATION ISO/CEI 27001 LEAD IMPLEMENTER

PECB

Ce séminaire 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 l'Information (SMSI) conforme à la norme ISO 27001. Cette formation est conçue de manière à doter d'une maîtrise des meilleures pratiques en matière de Système 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/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.

Code et durée :
- 27001-LI
- 5 jours

Cibles :
- RSSI, DSI, Architectes,
- Chefs de projets, Avant-ventes,
- Administrateurs système & réseau,
- Experts sécurité,
- Consultants sécurité

Prérequis
- Connaissances de base de la sécurité informatique
- Base en qualité

OBJECTIFS PEDAGOGIQUES

- Comprendre la corrélation entre la norme ISO/CEI 27001 et la norme ISO/CEI 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/CEI 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

PROGRAMME DE FORMATION

- Jour 1 : Introduction à la norme ISO/CE et initialisation d'un SMSI
- Jour 2 : Planification de la mise en œuvre d'un SMSI
- Jour 3 : Mise en œuvre d'un SMSI
- Jour 4 : Surveillance, mesure, amélioration continue et préparation de l'audit de certification du SMSI
- Jour 5 : Examen de certification

EXAMEN

- Domaine 1 : Fondamentaux du SMSI ;
- Domaine 2 : Le SMSI ;
- Domaine 3 : Planification de la mise en œuvre d'un SMSI selon la norme ISO/CEI 27001 ;
- Domaine 4 : Mise en œuvre d'un SMSI conforme à la norme ISO/CEI 27001 ;
- Domaine 5 : Évaluation de la performance, surveillance et mesure d'un SMSI selon la norme ISO/CEI 27001 ;
- Domaine 6 : Amélioration continue d'un SMSI selon la norme ISO/CEI 27001 ;
- Domaine 7 : Préparation de l'audit de certification d'un SMSI.

CERTIFICATION ISO/CEI 27001 LEAD AUDITOR

PECB

Au cours de ce séminaire, 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 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.

Code et durée :
- 27001-LA
- 5 jours

Cibles :
- Auditeurs ;
- RSSI, DSI ;
- Responsables conformité SMSI ;
- Chefs de projets, Avant-ventes ;
- Experts sécurité ;
- Consultants sécurité.

Prérequis :
- Une bonne connaissance de la norme ISO/CEI 27001 ;
- Et des connaissances approfondies sur les principes de l'audit ;

OBJECTIFS PEDAGOGIQUES

- Comprendre le fonctionnement d'un Système de management de la sécurité de l'information (SMSI) conforme à la norme ISO /CEI 27001 ;
- Expliquer la corrélation entre la norme ISO/CEI 27001 et la norme ISO/CEI 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/CEI 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 ;
- Acquérir les connaissances des normes nécessaires aux certifications ISO 27001 Lead Auditor.

PROGRAMME DE FORMATION

- Jour 1 : Introduction au SMSI et à la norme ISO/CEI 27001
- Jour 2 : Principes, préparation et déclenchement de l'audit
- Jour 3 : Activités d'audit sur site
- Jour 4 : Clôture de l'audit
- Jour 5 : Examen de certification

EXAMEN

L'examen « PECB Certified ISO/CEI 27001 Lead Auditor » remplit les exigences relatives au programme d'examen et de certification de PECB. L'examen couvre les domaines de compétences suivants :

- Domaine 1 : Fondamentaux du SMSI ;
- Domaine 2 : SMSI ;
- Domaine 3 : Fondamentaux de l'audit ;
- Domaine 4 : Préparation d'un audit ISO/CEI 27001 ;
- Domaine 5 : Réalisation d'un audit ISO/CEI 27001 ;
- Domaine 6 : Clôturer un audit ISO/CEI 27001 ;
- Domaine 7 : Gérer un programme d'audit ISO/CEI 27001.

CERTIFICATION ISO/CEI 27005 RISK MANAGER

PECB

Le séminaire « 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.

Code et durée :
- 27005-RM
- 3 jours

Cibles :
- RSI,
- Membres d'une équipe de SI ;
- Responsable de SI, de la conformité et du risque dans un organisation ;
- Tout individu mettant en œuvre la norme ISO/CEI 27001, désirant se conformer à elle ou impliqué dans un programme de management des risques.
- Consultants des TI ; Professionnels des TI
- Agents de SI

Prérequis
- Une compréhension fondamentale de la norme ISO/IEC 27005 ;
- Et une connaissance approfondie de l'évaluation des risques et de la SI.

OBJECTIFS PEDAGOGIQUES

- 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.

PROGRAMME DE FORMATION

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

EXAMEN

L'examen « PECB Certified ISO/IEC 27005 Risk Manager » remplit les exigences relatives au programme d'examen et de certification de PECB. L'examen couvre les domaines de compétences suivants :

- Domaine 1 : Principes et concepts fondamentaux relatifs à la gestion des risques liés à la sécurité de l'information ;
- Domaine 2 : Mettre en œuvre un programme de gestion des risques liés à la sécurité de l'information ;
- Domaine 3 : Processus et cadre de gestion des risques liés à la sécurité de l'information conformes à la norme ISO/IEC 27005 ;
- Domaine 4 : Autres méthodes d'appréciation des risques de la sécurité de l'information.

CERTIFICATION ISO/CEI 22301 LEAD AUDITOR

Le séminaire ISO 22301 Lead Auditor vous permettra d'acquérir l'expertise nécessaire pour réaliser des audits de Système de management de la continuité d'activité (SMCA) en appliquant les principes, les procédures et les techniques d'audit généralement reconnues. Durant cette formation, vous acquerrez les connaissances et les compétences nécessaires pour planifier et réaliser des audits internes et externes, en conformité avec la norme ISO 19011 et le processus de certification d'ISO/CEI 17021-1.

Grâce aux exercices pratiques, vous serez en mesure de maîtriser les techniques d'audit et disposerez des compétences requises pour gérer un programme d'audit, une équipe d'audit, la communication avec les clients et la résolution de conflits.

Après avoir acquis l'expertise nécessaire pour réaliser cet audit, vous pouvez vous présenter à l'examen et postuler au titre de « PECB Certified ISO 22301 Lead Auditor ». Le certificat PECB atteste que vous avez acquis les capacités nécessaires pour l'audit des organisations selon les meilleures pratiques d'audit.

Code et durée :
- 22301-LA
- 5 jours

Cibles :
- Auditeurs souhaitant réaliser et diriger des audits de certification du SMCA ;
- Responsables ou consultants désirant maîtriser le processus d'audit du SMCA ;
- Toute personne responsable du maintien de la conformité aux exigences du SMCA ;
- Experts techniques désirant préparer un audit du SMCA ;
- Conseillers spécialisés en MCA.

Prérequis
- Une bonne connaissance de la norme ISO 22301 ;
- Et des connaissances approfondies sur les principes de l'audit.

OBJECTIFS PEDAGOGIQUES

- 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.

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 ;
- Jour 5 : Examen de certification.

EXAMEN

L'examen « PECB Certified ISO 22301 Lead Auditor » remplit les exigences relatives au programme d'examen et de certification de PECB. L'examen couvre les domaines de compétences suivants :

- Domaine 1 : Principes et concepts fondamentaux du Système de management de la continuité d'activité
- Domaine 2 : Système de management de la continuité d'activité (SMCA)
- Domaine 3 : Principes et concepts fondamentaux de l'audit
- Domaine 4 : Préparation d'un audit ISO 22301
- Domaine 5 : Réalisation d'un audit ISO 22301
- Domaine 6 : Clôturer un audit ISO 22301
- Domaine 7 : Gérer un programme d'audit ISO 22301
- SMSI

CERTIFICATION ISO/CEI 22301 LEAD IMPLEMENTER

Le séminaire 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.

Code et durée :
- 22301-LI
- 5 jours

Cibles :
- Responsables ou consultants impliqués dans le MCA ;
- Conseillers spécialisés désirant maîtriser la mise en œuvre d'un SMCA ;
- 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.

OBJECTIFS PEDAGOGIQUES

- 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

PROGRAMME

- Jour 1 : Introduction à la norme ISO/CE et initialisation d'un SMSI
- Jour 2 : Planification de la mise en œuvre d'un SMSI
- Jour 3 : Mise en œuvre d'un SMSI
- Jour 4 : Surveillance, mesure, amélioration continue et préparation de l'audit de certification du SMSI
- Jour 5 : Examen de certification

EXAMEN

L'examen « PECB Certified ISO 22301 Lead Implementer » remplit les exigences relatives au programme d'examen et de certification de PECB. L'examen couvre les domaines de compétences suivants :

- Domaine 1 : Fondamentaux du SMCA.
- Domaine 2 : SMCA
- Domaine 3 : Planification de la mise en œuvre d'un SMCA conforme à la norme ISO 22301
- Domaine 4 : Mise en œuvre d'un SMCA conforme à la norme ISO 22301
- Domaine 5 : Évaluation de la performance, surveillance et mesure d'un SMCA conforme à la norme ISO 22301
- Domaine 6 : Amélioration continue d'un SMCA conforme à la norme ISO 22301
- Domaine 7 : Préparation de l'audit de certification d'un SMCA ;

CERTIFICATION ISO/CEI 22301 LEAD IMPLEMENTER

PECB

Le séminaire 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.

Code et durée :

- 22301-LI
- 5 jours

Cibles :

- Responsables ou consultants impliqués dans le MCA ;
- Conseillers spécialisés désirant maîtriser la mise en œuvre d'un SMCA ;
- 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.

OBJECTIFS PEDAGOGIQUES

- 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

PROGRAMME

- Jour 1 : Introduction à la norme ISO/CE et initialisation d'un SMSI
- Jour 2 : Planification de la mise en œuvre d'un SMSI
- Jour 3 : Mise en œuvre d'un SMSI
- Jour 4 : Surveillance, mesure, amélioration continue et préparation de l'audit de certification du SMSI
- Jour 5 : Examen de certification

EXAMEN

L'examen « PECB Certified ISO 22301 Lead Implementer » remplit les exigences relatives au programme d'examen et de certification de PECB. L'examen couvre les domaines de compétences suivants :

- Domaine 1 : Fondamentaux du SMCA.
- Domaine 2 : SMCA
- Domaine 3 : Planification de la mise en œuvre d'un SMCA conforme à la norme ISO 22301
- Domaine 4 : Mise en œuvre d'un SMCA conforme à la norme ISO 22301
- Domaine 5 : Évaluation de la performance, surveillance et mesure d'un SMCA conforme à la norme ISO 22301
- Domaine 6 : Amélioration continue d'un SMCA conforme à la norme ISO 22301
- Domaine 7 : Préparation de l'audit de certification d'un SMCA ;

CERTIFICATION ISO 27001 LEAD IMPLEMENTER

Ce séminaire est composé du tronc commun permettant de donner le socle théorique commun aux certifications ISO 27001 Lead Auditor et ISO 27001 Lead Implementer suivi du stage de préparation à l'examen de certification Lead Implementer (ILI). Ce dernier a pour objectif de réviser les connaissances nécessaires à la certification et vous préparer au passage de l'examen. Il se termine par l'examen proprement dit.

L'examen certifie que vous possédez les connaissances et les compétences nécessaires pour implémenter un SMSI suivant la norme ISO/IEC 27001 :2013. Cet examen est dirigé par LSTI (accrédité COFRAC).

Code et durée :

- 27001+ ILI
- 5 jours

Cibles :

- RSSI, DSI, Architectes,
- Chefs de projets, Avant-ventes,
- Administrateurs système & réseau,
- Experts sécurité,
- Consultants sécurité

Prérequis :

- Connaissances de base de la sécurité informatique
- Base en qualité

OBJECTIFS PEDAGOGIQUES

- Acquérir les connaissances des normes nécessaires aux certifications ISO 27001 Lead Auditor
- Acquérir la démarche de mise de l'audit du SMSI
- Révision des normes nécessaires à la certification
- Exercices de préparation à l'examen de certification

PROGRAMME

Le tronc commun : ISO

- Introduction
- Les normes ISO 2700x
- La norme ISO 27001:2013
- Les bonnes pratiques, référentiel ISO 27002:2013
- La mise en œuvre de la sécurité dans un projet SMSI
- Les audits de sécurité ISO 19011:2018
- Les organismes de certification - ISO 17021:2015
- Les bonnes pratiques juridiques
- La certification ISO de la sécurité du SI : La relation auditeur-audité

Préparation à l'examen : ILI

- Travaux dirigés
- Corrections collectives
- Révision finale
- Examen

CERTIFICATION ISO/CEI 27001 LEAD AUDITOR

Ce séminaire est composé du tronc commun permettant de donner le socle théorique commun aux certifications ISO 27001 Lead Auditor et ISO 27001 Lead Implementer suivi du stage de préparation à l'examen de certification Lead Implementer (ILA). Ce dernier a pour objectif de réviser les connaissances nécessaires à la certification et vous préparer au passage de l'examen. Il se termine par l'examen proprement dit.

L'examen certifie que vous possédez les connaissances et les compétences nécessaires pour auditer un SMSI suivant la norme ISO/IEC 27001 : 2013. Cet examen est dirigé par LSTI (accrédité COFRAC).

Code et durée :

- 27001+ ILA
- 5 jours

Cibles :

- RSSI, DSI, Architectes,
- Chefs de projets, Avant-ventes,
- Administrateurs système & réseau,
- Experts sécurité,
- Consultants sécurité

Prérequis

- Connaissances de base de la sécurité informatique
- Base en qualité

OBJECTIFS PEDAGOGIQUES

- Acquérir les connaissances des normes nécessaires aux certifications ISO 27001 Lead Auditor
- Acquérir la démarche de mise de l'audit du SMSI
- Révision des normes nécessaires à la certification
- Exercices de préparation à l'examen de certification

PROGRAMME

Le tronc commun : ISO

- Introduction
- Les normes ISO 2700x
- La norme ISO 27001 : 2013
- Les bonnes pratiques, référentiel ISO 27002 : 2013
- La mise en œuvre de la sécurité dans un projet SMSI
- Les audits de sécurité ISO 19011 : 2018
- Les organismes de certification - ISO 17021 : 2015
- Les bonnes pratiques juridiques
- La certification ISO de la sécurité du SI : La relation auditeur-audité.

Préparation à l'examen : ILA

- Travaux dirigés
- Corrections collectives
- Révision finale
- Examen

CISSP, PREPARATION A LA CERTIFICATION SECURITE (ISC)²

Ce stage détaille les concepts de sécurité pour l'obtention de la certification CISSP. Il vous préparera au passage de l'examen en couvrant l'ensemble du Common Body of Knowledge (CBK), le tronc commun de connaissances en sécurité défini par l'International Information Systems Security Certification Consortium (ISC)².

Pour passer la certification, vous devez vous inscrire sur le site de l'ISC2 et déposer un dossier d'éligibilité.

Code et durée :

- CISSP
- 5 jours

Cibles :

- RSSI,
- Consultants sécurité
- Experts sécurité

Prérequis :

- Connaissances de base sur les réseaux et les systèmes d'exploitation
- Connaissance de base à la sécurité de l'information
- Connaissances de base des normes en audit et en continuité des affaires.

OBJECTIFS PEDAGOGIQUES

- Connaître le Common Body of Knowledge de la sécurité IT
- Développer une vision globale des enjeux de sécurité IT
- Approfondir les connaissances des huit domaines du CISSP
- Se préparer à l'examen de certification du CISSP

PROGRAMME

- Sécurité du SI et le CBK de l'(ISC)²
  - La sécurité des Systèmes d'Information.
  - Le pourquoi de la certification CISSP.
  - Présentation du périmètre couvert par le CBK.
- Gestion de la sécurité et sécurité des opérations
  - Pratiques de gestion de la sécurité. La rédaction de politiques, directives, procédures et standards en sécurité.
  - Le programme de sensibilisation à la sécurité, pratiques de management, gestion des risques, etc.
  - Sécurité des opérations : mesures préventives, de détection et correctives, rôles et responsabilités des acteurs.
  - Les meilleures pratiques, la sécurité lors de l'embauche du personnel, …
- Architecture, modèles de sécurité et contrôle d'accès
  - Architecture et modèles de sécurité : architecture de système, modèles théoriques de sécurité de l'information.
  - Les méthodes d'évaluation de systèmes, modes de sécurité opérationnels, etc.
  - Systèmes et méthodologies de contrôle d'accès. Les catégories et types de contrôles d'accès.
  - Accès aux données et aux systèmes, systèmes de prévention des intrusions (IPS) et de détection d'intrusions (IDS).
  - Journaux d'audit, menaces et attaques reliées au contrôle des accès, …
- Cryptographie et sécurité des développements
  - Cryptographie. Les concepts, cryptographie symétrique et asymétrique.
  - Les fonctions de hachage, infrastructure à clé publique, etc.
  - Sécurité des développements d'applications et de systèmes. Les bases de données, entrepôts de données.
  - Le cycle de développement, programmation orientée objet, systèmes experts, intelligence artificielle, etc.
- Sécurité des télécoms et des réseaux
  - Sécurité des réseaux et télécoms. Les notions de base, modèle TCP/IP, équipements réseaux et de sécurité.
  - Les protocoles de sécurité, les attaques sur les réseaux, sauvegardes des données, technologies sans fil, VPN ...
- Continuité des activités, loi, éthique et sécurité physique
  - Continuité des opérations et plan de reprise en cas de désastre.
  - Le plan de continuité des activités, le plan de rétablissement après sinistre.
  - Les mesures d'urgence, programme de formation et de sensibilisation, communication de crise, exercices et tests.
  - Loi, investigations et éthique : droit civil, criminel et administratif, propriété intellectuelle.
  - Le cadre juridique en matière d'investigation, règles d'admissibilité des preuves, etc.
  - La sécurité physique. Les menaces et vulnérabilités liées à l'environnement d'un lieu, périmètre de sécurité.

CYBERSECURITE DES RESEAUX - SYNTHESE

Ce séminaire vous montre comment répondre aux impératifs de sécurité des entreprises et intégrer la sécurité dans l'architecture d'un système d'information. Il comprend une analyse détaillée des menaces et moyens d'intrusion ainsi qu'un panorama des principales mesures de sécurité disponibles sur le marché.

A l'issue de ce séminaire, vous disposerez des éléments techniques et juridiques pour comprendre comment assurer et superviser la sécurité de votre système d'information.

Code et durée :

- CRI
- 3 jours

Cibles :

- RSSI, DSI, architectes,
- Chefs de projets, Commerciaux avant-ventes,
- Administrateurs système & réseau.
- Experts sécurité
- Consultants sécurité

Prérequis :

- Connaissances générales en informatique
- Connaissance en réseau Internet.

OBJECTIFS PEDAGOGIQUES

- Connaître l'évolution de la cybercriminalité et de ses enjeux
- Maîtriser la sécurité du Cloud, des applications, des postes clients
- Comprendre les principes de la cryptographie

PROGRAMME

- Sécurité de l'information et cybercriminalité
- Firewall réseaux, Firewall applicatifs
- Sécurité des postes clients
- Fondamentaux de la cryptographie
- Authentification et habilitation des utilisateurs
- La sécurité des flux
- Sécurité Wifi
- Sécurité des Smartphones
- Sécurité des applications
- Gestion et supervision active de la sécurité

SECURITE SYSTEME RESEAUX

Ce stage pratique vous montrera comment mettre en œuvre les principaux moyens de sécurisation des systèmes et des réseaux. Après avoir étudié quelques menaces pesant sur le système d'information,

Vous apprendrez le rôle des divers équipements de sécurité dans la protection de l'entreprise afin d'être en mesure de concevoir une architecture de sécurité et de réaliser sa mise en œuvre.

Les concepts théoriques vus seront mis en œuvre lors de stage pratique.

Code et durée :

- SSR
- 3 jours

Cibles :

- Architectes,
- Administrateurs système & réseau.
- Experts sécurité
- Consultants sécurité

Prérequis :

- Connaissance en systèmes et réseaux

OBJECTIFS PEDAGOGIQUES

- Connaître les failles et les menaces des systèmes d'information
- Maîtriser le rôle des divers équipements de sécurité
- Concevoir et réaliser une architecture de sécurité adaptée
- Mettre en œuvre les principaux moyens de sécurisation des réseaux
- Utiliser des outils de détection de vulnérabilités

PROGRAMME

- Architectures de sécurité
- Sécurité des données
- Sécurité des échanges
- Sécuriser un système, le "Hardening"
- Audit et sécurité au quotidien
- Étude de cas
- Exercices pratiques :

- Utilisation des lacunes protocolaires : Man In The Middle, Craquage de mots de passe, …
- Installation et configuration d'un serveur SSH
- Manipulation des objets cryptographiques (algorithmes, fonctions de hachage, clés, …)
- Magasins de certificats Microsoft. Mettre en œuvre la signature et le chiffrement de messages.
- Mise en œuvre d'une autorité de certification racine. Génération de certificats utilisateurs et serveurs.
- Mise en œuvre d'une hiérarchie d'autorités de certification (autorité racine, autorités intermédiaires, …).

SECURITE DES APPLICATIONS WEB

L'intrusion sur les serveurs de l'entreprise représente un risque majeur. Il est essentiel de comprendre et d'appliquer les technologies et les produits permettant d'apporter le niveau de sécurité suffisant aux applications déployées et plus particulièrement aux applications à risque comme les services extranet et la messagerie.

Résolument pragmatique, ce stage vous apportera les clés de la protection d'un service en ligne à partir d'exemples concrets d'attaques et de ripostes adaptées

Code et durée :

- SAW
- 3 jours

Cibles :

- Développeurs / Webmaster
- Administrateurs réseaux, systèmes
- Experts sécurité
- Consultants sécurité

Prérequis :

- Connaissances développement des applications web

OBJECTIFS PEDAGOGIQUES

- Identifier les vulnérabilités les plus courantes des applications Web
- Comprendre le déroulement d'une attaque
- Tester la sécurité de ses applications Web
- Configurer un serveur Web pour chiffrer le trafic Web avec HTTPS
- Mettre en place des mesures de sécurisation simples pour les applications Web

PROGRAMME

- Constituants d'une application Web
- Le protocole HTTP en détail
- Les vulnérabilités des applications Web
- Le firewall réseau dans la protection d'applications HTTP
- Sécurisation des flux avec SSL/TLS
- Configuration du système et des logiciels
- Principe du développement sécurisé
- L'authentification des utilisateurs
- Le firewall "applicatif"
- Exercices pratiques :
- Utilisation de l'analyseur réseau Wireshark.
- Utilisation d'un proxy d'analyse HTTP spécifique.
- Attaque Cross Site Scripting. Exploitation d'une faille sur le frontal http.
- Contournement d'une authentification par injection de requête SQL.
- Mise en œuvre de SSL sous IIS et Apache. Attaques sur les flux HTTPS avec sslstrip et sslsnif.
- Procédure de sécurisation du frontal Web (Apache ou IIS).
- Mise en œuvre d'un firewall applicatif. Gestion de la politique de sécurité. Attaques et résultats.

TEMOIGNAGES DE NOS CLIENTS

« Malick réalise des prestations de conseil en sécurité de très grande qualité. Les échanges sont enrichissants et ses observations toujours pertinentes.
De plus, c'est un très bon formateur. Un très bon pédagogue, qui s'investit énormément et m'a permis d'obtenir la certification ISO 27001 Implementer. » Florent C., Cloud Security Officer chez Cegid

« *Merci Malick ! J'ai découvert le professionnalisme et la pertinence d'un auditeur ISO doublés d'un rapport humain de valeur. J'ai apprécié la qualité d'analyse et l'écoute. Bravo pour la précision et l'acuité des recommandations ! Autant de savoir-faire et de compétences qui installent une vraie confiance* ». Jean D., Directeur projet chez Orange

« *Malick est un bon professionnel et grâce à son niveau d'expertise très élevé, c'est avec assurance qu'on peut lui confier des projets d'envergure.* » Giuseppe D., Directeur Grands Projets chez Orsys

« *J'ai eu l'occasion fin juin 2018 de suivre le cours de préparation à la certification ISO 27001 Lead Implementer animé par Malick dans les locaux d'Orsys. Malick maitrise parfaitement la norme ISO 27001, les différentes solutions de Sécurité du SI mais sait aussi rester pragmatique, les solutions de SSI n'étant pas forcément les mêmes en fonction de la taille ou du secteur des entreprises ou organisations. Cherry on the cake, j'ai réussi la certification LSTI ISO 27001 Lead Implementer ! Merci Malick !* », Pierre J., Directeur Qualité Groupe Astek – Resp. Environnement et RSE - CSSI

« *Malick est un formateur très pédagogue. Grâce à sa méthodologie de préparation j'ai pu passer ma certification 27001 Lead auditor au premier essai sans difficultés. Merci Malick FALL* » Lesly D., Cyber Security Consultant chez Davidson consulting

« *J'ai été stagiaire de Malick lors de la formation ISO 27001 : 2013 Lead Auditor, plus particulièrement lors de la phase de préparation. Malick maîtrise le sujet et est un bon formateur avec qui il est aisé d'échanger. La préparation s'est très bien passée d'autant plus que j'ai réussi l'examen !* », Franck D., Ingénieur sécurité et normalisation chez Worldline Global

« *J'ai eu le privilège d'être un des étudiants de Malick, en sécurité des infrastructures, dans le cadre de mon mastère. Il faut avouer que Malick se démarque par ses qualités professionnelles et humaines. C'est un expert en cyber sécurité, en audit et en conformité, mais aussi, un conseiller chevronné qui sait bien allier la technique, la communication et le management. Je souhaite aussi souligner que c'est un homme d'honneur, intègre.* », Yassine R., IT Director & ITSO chez Atos Maroc

« *Malick fut un très bon formateur, on sent chez lui l'expertise et la maîtrise du sujet (sécurité réseaux et systèmes). Le courant est très bien passé entre lui et nous, il y eut une très bonne ambiance.* » Vincent C., Technicien Systèmes et applicatifs à la mairie de Saint-Laurent-Du-Var

« Si je devais décrire Malick Fall en quelques mots, moi dont le cœur de métier est de repérer les compétences : Il allie sérieux, responsabilité, grandes capacités d'analyses et de synthèse, rapidité d'exécution, pédagogie dans sa façon de rassurer l'apprenant et de lui transmettre les savoirs faire. Je le recommande absolument !... Pas pour lui… pour vous, pour votre entreprise. Ce qu'il peut vous transmettre va permettre à votre entreprise d'être plus performante. » Evelyne W., Fondateur et General Manager du cabinet W Talent Management

POLARIS
SECURE TECHNOLOGIES

AUDIT - CONSEIL - FORMATION
EN CYBERSECURITE

FRANCE

37 RUE D'ALSACE 69800 ST-PRIEST

+33 4 78 74 50 80 / +33 7 86 00 47 79

SÉNÉGAL

LIBERTÉ 6 EXT BP 21207 DAKAR PONTY

+221 77 778 10 10 / +221 33 867 25 30

contact@polaris-st.com

www.polaris-st.com