NL CONSULTING

Certification des Professionnels de la Sécurité des Systèmes d'Information et de l'Audit

---

Catalogue de formation

Sécurité des Systèmes d'Information et Audit V1.0

http://www.nl-consulting.fr

Siege Social
2, rue du Colonel Dominé 75013 Paris

Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

Qui sommes-nous ?

NL CONSULTING est un organisme de formation en Sécurité des Systèmes d'Information et Audit **agréé** par **PECB** et par **MILE2**.

En partant d'une analyse des menaces et des risques, nous avons élaboré un portefeuille de formations les plus complémentaires possibles en matière de Sécurité des Systèmes d'information et d'Audit afin de vous apporter les connaissances nécessaires à la maîtrise des normes internationales dans ces domaines, et vous préparer aux certifications professionnelles associées :

- **CISSO/CISSP** (Certified Information Systems Security Professional) [Réf : CISOP]
- **PECB Certified Lead Auditor : ISO 27001 : 2013 (SMSI)** [Réf : LAISO]
- **PECB Certified Lead Implementer : ISO 27001 : 2013 (SMSI)** [Réf : LIISO]
- **PECB Certified Risk Manager: ISO 27005 : 2011** [Réf : RMISO]
- **PECB Certified Risk Manager : EBIOS** [Réf : RMEBI]
- **PECB Certified Risk Manager ISO 27005 avec la méthode EBIOS** [Réf : RMISE]
- **PECB Certified Risk Manager : MEHARI** [Réf : RMMEH]
- **PECB Certified Lead Cybersecurity Manager ISO 27032** [Réf : LCISO]
- **PECB Certified Lead Implementer : ISO 22301 : 2012 (SMCA)** [Réf : LISMC]
- **CISM** (Certified Information Security Manager) [Réf : CCISM]
- **CISA** (Certified Information Systems Auditor) [Réf : CCISA]
- **CPEH** (Certified Professional Ethical Hacker) [Réf : CCPEH]
- **Maîtriser le processus d'élaboration d'une PSSI** [Réf : MPSSI]
- **Maîtriser le processus d'élaboration d'un TdB SSI** [Réf : MTBSI]
- **Cryptographie** [Réf : CRYPT]

Siege Social
2, rue du Colonel Dominé 75013 Paris

Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

Pourquoi être certifié en Sécurité des Systèmes d'Information et Audit ?

Quel que soit leur domaine d'expertise et durant toute leur carrière professionnelle tous les Ingénieurs et Managers sont confrontés au même challenge : « **Maintenir leurs compétences au meilleur niveau** ».

Dans un monde fortement exposé aux menaces de sécurité, le besoin en professionnels de la Sécurité des Systèmes d'Information et de l'Audit bien informés et compétents n'a jamais été aussi grand. Votre expérience dans ce domaine est une composante importante de votre valeur ajoutée à votre employeur mais elle n'est pas suffisante. En effet, les employeurs ont besoin de quelque chose de quantifiable et de vérifiable pour leur montrer que vous avez l'expertise qu'ils recherchent. Une certification par un organisme internationalement reconnu est devenue indispensable à tout professionnel de la Sécurité des Systèmes d'Information et de l'Audit.

Actuellement les postes dans beaucoup d'organismes privées ou publics requièrent une certification et les praticiens certifiés de la Sécurité des Systèmes d'Information et de l'Audit disposent de revenus potentiellement plus élevés et d'opportunités de carrière plus importantes.

De plus vous serez reconnu comme quelqu'un de sérieux, de professionnel appartenant aux grandes familles des professionnels de la Sécurité des Systèmes d'Information et de l'Audit.

Comment **NL CONSULTING** peut-elle vous aider à devenir un Expert reconnu dans votre profession ?

Nos formations préparatoires aux certifications professionnelles en Sécurité des Systèmes d'Information et Audit s'adressent à tous ceux qui ont à gérer la Sécurité des Systèmes d'Information au quotidien : conduire une analyse de risques, définir une politique de sécurité et de continuité, la décliner par une organisation et des solutions adaptées comme à auditer un système existant.

Les avantages des formations préparatoires aux certifications professionnelles en Sécurité des Systèmes d'Information et Audit proposées par **NL CONSULTING** sont ?

- L'amélioration de la crédibilité professionnelle et la reconnaissance internationale,
- L'accélération de la carrière professionnelle,
- L'aide au recrutement.

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

A qui s'adressent les formations NL CONSULTING ?

Nos formations sont destinées aux informaticiens (DSI, Managers, Ingénieurs, Experts Consultants, Chefs de Projets), Ingénieurs Sécurité, RSSI, Consultants Sécurité, Risk Managers, Auditeurs.

Elles sont accessibles soit en **mode inter - entreprises** soit en **mode intra – entreprise** et sont animées par des Experts Seniors certifiés CISSP, CISSO, CISA, CISM, CBCP, CEH, CPEH, CPTE, Lead Implementer ISO 27001, Lead Auditor ISO 27001, Risk Manager ISO 27005, Risk Manager EBIOS, Risk Manager MEHARI.

NL CONSULTING peut vous guider dans le choix de la formation la mieux adaptée à vos attentes et vous accompagner pour la réussir.

Nous sommes à votre disposition pour tout renseignement complémentaire.

Contact, information, devis, inscription :

E-mail : **nlabani@nl-consulting.fr**
Tél : +33 6 25 57 58 14
Site web : **http://www.nl-consulting.fr**

CISSO/CISSP

(Certified Information Systems Security Professional)

[Réf : CISOP]

Cette formation a pour but de préparer les candidats à l'examen du **CISSO** (Certified Information Systems Security Officer), la certification internationale délivrée par **MILE2**.

La formation CISSO couvre l'ensemble des connaissances en sécurité de l'information dans les domaines suivants : **Management du risque et de la sécurité, Sécurité des actifs, Sécurité de l'Engineering, Cryptographie, Sécurité des réseaux et des communications, Management des Identités et des Accès, Evaluation et test de la sécurité, Sécurité du développement logiciel, Sécurité des opérations, Continuité des activités et reprise d'activité, Sécurité physique, Conformité**.

La formation CISSO est à l'heure actuelle la formation la plus à jour et la plus pratique dans le monde. Elle est alignée sur les objectifs des standards majeurs ISO27001, NIST, CISM et CISSP.

La formation CISSO permet donc pour ceux qui le souhaitent des se présenter ultérieurement et de passer plus facilement l'examen de certification CISSP organisée par (ISC)².

Tout au cours de la semaine, les participants sont invités à répondre à des questions, en groupe et individuellement, sur chacun des domaines et similaires à l'examen officiel.

Attention :

- L'examen se fait sur le site de MILE2 **(http://www.mile2.com)** a lieu l'après-midi du 5e jour.

Objectifs :

- Acquérir les connaissances nécessaires à la réussite des examens CISSO et CISSP® ;
- Maîtriser les connaissances en sécurité de l'information dans les domaines du tronc commun de connaissances ;
- Comprendre les besoins en sécurité de l'information pour toute l'organisation ;

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

- Acquérir les connaissances nécessaires pour conseiller une organisation sur les meilleures pratiques en management de la sécurité de l'information.

Participants :
Auditeurs confirmés ou informaticiens (DSI, RSSI, Managers, Ingénieurs, Experts Consultants) qui souhaitent obtenir la certification CISSO (Certified Information System Security Officer) délivrée par MILE2, et se présenter à l'examen à l'issue de la formation.

Pour ceux qui le souhaitent, la formation permet également de se présenter ultérieurement à l'examen de certification CISSP organisée par (ISC)².

Pré -requis :

- Une expérience dans le domaine des réseaux et de la sécurité ;
- La compréhension de l'anglais technique est nécessaire car le support de cours fourni aux participants est en anglais.

Bénéfices attendus de la formation :

- Reconnaissance Internationale des compétences en sécurité de l'information,
- Savoir dialoguer avec le management pour la mise en oeuvre des mesures de sécurité,
- Appréhender le rôle du RSSI dans l'organisation.

Intervenants :

- Les sessions sont animées par des Experts Seniors certifiés CISSP, CISSO,CISA, CISM, CBCP, CEH, CPEH, CPTE, CEH v8, Lead Auditor ISO 27001, Lead Implementer ISO 27001, Risk Manager ISO 27005, Risk Manager EBIOS, Risk Manager MEHARI.

Mode :

Formation inter – entreprises.

Programme :

Le programme de la formation suit les domaines couverts par l'examen :

Jour 1 :

- Domaine 1 : Management du risque et de la sécurité
- Domaine 2 : Sécurité des actifs

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

- Domaine 3 : Sécurité de l'Engineering
- Domaine 4 : Cryptographie

Jour 2 :

- Domaine 5 : Sécurité des réseaux et des communications
- Domaine 6 : Management des Identités et des Accès

Jour 3 :

- Domaine 7 : Evaluation et test de la sécurité
- Domaine 8 : Sécurité du développement logiciel
- Domaine 9 : Sécurité des opérations

Jour 4 :

- Domaine 10 : Continuité des Activités et Reprise d'Activité
- Domaine 11 : Sécurité physique
- Domaine 12 : Conformité

Jour 5 :

- Examen blanc (125 questions)
- **Examen de certification CISSO (après-midi)**

  - Examen de certification en ligne sur le site de MILE2 (durée 2 heures – 100 questions) ;
  - Condition de réussite : au moins 700 points de bonnes réponses ;
  - Résultat immédiat en fin d'examen avec envoi immédiat par e-mail du certificat CISSO en cas de réussite à l'examen.

Dans chaque exposé, l'accent sera mis sur les éléments organisationnels et technologiques fondamentaux.

Méthode :

- Ensemble d'exposés couvrant chaque domaine du programme de l'examen,

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

- A la fin de chaque exposé, les participants doivent s'entraîner à répondre à un ensemble de questions portant sur le thème de l'exposé. Ces questions sont issues des précédentes sessions du CISSO/CISSP (ou d'examens comparables),
- Simulation partielle de l'examen (examen blanc) effectuée en fin de formation.

Lieu d'examen :

- Site http://www.mile2.com

Durée : 5 jours.

Tarif : Nous consulter

- **Les frais d'examen CISSO sont compris dans le prix de cette session**,
- Le support de formation CISSO/CISSP en français est remis au démarrage de la session de formation,
- Un certificat de participation de 35 CPE (Unités d'éducation continue /Continuing Professional Education) est remis aux participants en fin de formation.

Siege Social
2, rue du Colonel Dominé 75013 Paris

Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

PECB Certified Lead Auditor : ISO 27001 : 2013 (SMSI)

[Réf : LAISO]

La formation intensive de cinq jours permet aux participants d'acquérir les connaissances nécessaires et de développer l'expertise pour :

- planifier et effectuer des audits de la conformité d'un système de management de la sécurité de l'information par rapport aux exigences de la norme ISO/CEI 27001 : 2013;

- manager une équipe d'auditeurs en appliquant les principes, procédures et techniques d'audits communément reconnus.

A partir d'exercices pratiques basés sur un cas d'étude, le stagiaire sera mis en situation de développer les compétences (maîtrise des techniques d'audit) et les aptitudes (gestion d'équipes et d'un programme d'audit, communication avec les clients, résolution de conflits, etc.) nécessaires à la conduite d'un audit.
La formation est basée sur les lignes directrices d'audit de système de management (ISO/CEI 19011:2011) ainsi que les meilleures pratiques internationales d'audit. Elle se compose de :

- Cours magistraux illustrés de cas concrets,

- Exercices pratiques, réalisés seul ou en groupe (jeux de rôles), tirés de missions réelles, en lien direct avec la préparation à l'examen.

Objectifs:

- Comprendre les principes d'application de l'ISO/CEI 27001 : 2013 dans la construction d'un système de management de la sécurité de l'information,
- Comprendre la relation entre le système de management de la sécurité de l'information, le management des risques, les mesures, et les différentes parties prenantes,
- Comprendre les principes, procédures et techniques d'audit de l'ISO/CEI 19011 : 2011, et comment les appliquer dans le cadre d'un audit selon l'ISO/CEI 27001 : 2013,

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

- Comprendre l'application des obligations légales, statutaires, réglementaires ou contractuelles pertinentes lors de l'audit d'un SMSI,
- Acquérir les compétences nécessaires pour effectuer un audit de façon efficace, et les techniques de gestion d'une équipe d'audit, préparer et compléter un rapport d'audit ISO/CEI 27001 :2013.

Participants:

- Personnes désirant diriger des audits de certification ISO/CEI 27001 : 2013 en tant que responsable d'une équipe d'audit,
- Consultants désirant préparer et accompagner une organisation lors d'un audit de certification ISO/CEI 27001 : 2013,
- Auditeurs internes désirant préparer et accompagner leur organisation vers l'audit de certification ISO/CEI 27001 : 2013,
- Responsables de la sécurité de l'information ou de la conformité,
- Conseillers experts en technologies de l'information.

Pré-requis:

- Etre titulaire d'un diplôme de niveau Bac + 2 minimum ou justifier de 5 années d'expérience dans le domaine de la Sécurité des Systèmes d'information,

- Une connaissance préalable des normes ISO/CEI 27001 : 2013 et ISO/CEI 27002 : 2013 est recommandée,

- La compréhension de l'anglais est nécessaire car une partie de la documentation fournie aux participants est en anglais.

Bénéfices attendus de la formation :

- Reconnaissance Internationale des compétences et des connaissances pour auditer la conformité d'un SMSI à la norme ISO/IEC 27001 : 2013.
- Apporter d'une plus grande crédibilité dans la conduite de vos projets d'audit.

Intervenants :

- Les sessions sont animées par des Experts Seniors certifiés CISSP, CISSO, CISA, CISM, CBCP, CEH, CPEH, CPTE, Lead Auditor ISO 27001, Lead Implementer ISO 27001, Risk Manager ISO 27005, Risk Manager EBIOS, Risk Manager MEHARI.

Mode :

Formation inter – entreprises.

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

Programme :

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

- Cadre normatif, légal et réglementaire lié à la sécurité de l'information
- Principes fondamentaux de la sécurité de l'information
- Processus de certification ISO 27001
- Système de Management de la Sécurité de l'Information (SMSI)
- Présentation détaillée des clauses 5 à 10 de l'ISO 27001

Jour 2 : Planification et initialisation d'un audit 27001

- Principes et concepts fondamentaux d'audit
- Approche d'audit basée sur les preuves et sur le risque
- Préparation d'un audit de certification ISO 27001
- Audit documentaire d'un SMSI
- Conduire une réunion d'ouverture

Jour 3 : Conduire un audit ISO 27001

- Communication pendant l'audit
- Procédures d'audit : observation, revue documentaire, entretiens, techniques d'échantillonnage, vérification technique, corroboration et évaluation
- Rédaction des plans de tests d'audit
- Formulation des constats d'audit
- Rédaction des rapports de non-conformité

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

- Documentation d'audit
- Revue qualité
- Mener une réunion de clôture et fin d'un audit 27001
- Évaluation des plans d'action correctifs
- Audit de surveillance ISO 27001
- Programme de gestion d'audit interne ISO 27001

Jour 5 : Processus de certification ISO/CEI 27001 : 2013 et examen

- Processus de certification ;
- Examen de certification PECB Certified Lead Auditor ISO/CEI 27001 : 2013

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

Les résultats de l'examen vous parviendront par courrier environ six à huit semaines plus tard. L'examen Lead Auditor : ISO/CEI 27001 est disponible en français et dure 3 heures.
Le participant ayant réussi l'examen se verra délivrer une attestation de réussite. Pour réussir le participant devra obtenir un minimum de 70 points sur 100. Il sera qualifié de « Provisional Auditor » et disposera de 3 années pour demander à être certifié, selon son niveau d'activité, « Auditor ISO/CEI 27001 » ou « Lead Auditor ISO/CEI 27001».

Lieu d'examen :

- **Paris.**

Durée : 5 jours.

Tarif : Nous consulter

- Le coût de l'examen est **inclus** dans le tarif spécifique de cette formation,
- Les normes ISO/CEI 27001:2013, ISO/CEI 27002 : 2013 et ISO/CEI 19011:2011 de préparation à la certification Lead Auditor : ISO/CEI 27001 ainsi que le Support de formation sont fournis au démarrage de la session de formation,
- Un certificat de participation de 35 CPE (Unités d'éducation continue / Continuing Professional Education) est remis aux participants en fin de formation.

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

PECB Certified Lead Implementer : ISO 27001 : 2013 (SMSI)

[Réf : LIISO]

Cette formation a pour but de préparer les candidats à l'examen PECB Certified Lead Implementer ISO/CEI 27001 : 2013.

La formation intensive de cinq jours permet aux participants d'acquérir les connaissances nécessaires et de développer l'expertise pour :

- Conduire un projet d'implémentation d'un système de management de la sécurité de l'information satisfaisant aux exigences de la norme ISO/CEI 27001.

La formation se compose de :

- Cours magistraux illustrés de cas concrets,
- Exercices pratiques basé sur un cas d'étude, réalisés seul ou en groupe (jeux de rôles), tirés de missions réelles, en lien direct avec la préparation à l'examen.

Objectifs:

- Acquérir les connaissances relatives aux exigences de la norme ISO/CEI 27001 : 2013,
- Comprendre la relation entre le système de management de la sécurité de l'information, le management des risques, les mesures, et les différentes parties prenantes,
- Acquérir à travers une étude de cas les compétences nécessaires pour définir et implémenter un Système de Management de la Sécurité de l'Information conforme à la norme ISO/CEI 27001 : 2013.
- Obtenir la certification Lead Implementer ISO/CEI 27001 : 2013.

Siege Social
2, rue du Colonel Dominé 75013 Paris

Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

Participants:

- Consultants désirant préparer et accompagner une organisation pour l'implémentation d'un SMSI conforme à la norme ISO/CEI 27001 : 2013,
- Responsables de la Sécurité des Systèmes d'information ou de la Conformité,
- Conseillers experts en technologies de l'information.

Pré-requis:

- Etre titulaire d'un diplôme de niveau Bac + 2 minimum ou justifier de 5 années d'expérience dans le domaine de la Sécurité des Systèmes d'information,
- Une connaissance générale de la sécurité des systèmes d'information et de l'analyse des risques,
- Une connaissance préalable des normes ISO/CEI 27001 : 2013 et ISO/CEI 27002 : 2013 est recommandée,
- La compréhension de l'anglais est nécessaire car une partie de la documentation fournie aux participants est en anglais.

Bénéfices attendus de la formation :

- Reconnaissance Internationale des compétences et des connaissances pour implémenter un SMSI conforme à la norme ISO/IEC 27001 : 2013.

Intervenants :

- Les sessions sont animées par des Experts Seniors certifiés CISSP, CISSO, CISA, CISM, CBCP, CEH, CPEH, CPTE, Lead Auditor ISO 27001, Lead Implementer ISO 27001, Risk Manager ISO 27005, Risk Manager EBIOS, Risk Manager MEHARI.

Mode :

Formation inter – entreprises.

Programme :

Jour 1 : Introduction au concept de Système de Management de la Sécurité de l'Information (SMSI) tel que défini par l'ISO 27001; Initialisation d'un SMSI

- Introduction aux systèmes de management et à l'approche processus

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

- Présentation des normes ISO 27001, ISO 27002 et ISO 27003, ainsi que le cadre normatif, légal et réglementaire
- Principes fondamentaux de la sécurité de l'information
- Analyse préliminaire et détermination du niveau de maturité d'un système de management de sécurité de l'information existant d'après l'ISO 21827
- Rédaction d'une étude de faisabilité et d'un plan projet pour la mise en œuvre d'un SMSI

Jour 2 : Planifier la mise en œuvre d'un SMSI basé sur l'ISO 27001

- Définition du périmètre (domaine d'application) du SMSI
- Développement de la politique et des objectifs du SMSI
- Sélection de l'approche et de la méthode d'évaluation des risques
- Gestion des risques: identification, analyse et traitement du risque (d'après les dispositions de l'ISO 27005)
- Rédaction de la Déclaration d'Applicabilité

Jour 3 : Mettre en place un SMSI basé sur l'ISO 27001

- Mise en place d'une structure de gestion de la documentation
- Conception des mesures de sécurité et rédaction des procédures
- Implémentation des mesures de sécurité
- Développement d'un programme de formation et de sensibilisation, et communication à propos de la sécurité de l'information
- Gestion des incidents (d'après les dispositions de l'ISO 27035)
- Gestion des opérations d'un SMSI

Jour 4 : Contrôler, surveiller, mesurer et améliorer un SMSI ; audit de certification d'un SMSI

- Contrôler et surveiller un SMSI
- Développement de métriques, d'indicateurs de performance et de tableaux de bord conformes à l'ISO 27004
- Audit interne ISO 27001
- Revue de direction du SMSI
- Mise en œuvre d'un programme d'amélioration continue
- Préparation à l'audit de certification ISO 27001

Jour 5 : Processus de certification ISO/CEI 27001 : 2013 et examen

- Processus de certification ;
- Examen de certification PECB Certified Lead Implementer ISO/CEI 27001 : 2013 :

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

Les résultats de l'examen vous parviendront par courrier environ six à huit semaines plus tard. L'examen Lead Implementer ISO/CEI 27001 est disponible en français et dure 3 heures.
Le participant ayant réussi l'examen se verra délivrer une attestation de réussite. Pour réussir le participant devra obtenir un minimum de 70 points sur 100. Il sera qualifié de « Provisional Implementer » et disposera de 3 années pour demander à être certifié, selon son niveau d'activité, « Implementer ISO/CEI 27001 » ou « Lead Implementer ISO/CEI 27001».

Lieu d'examen :

- **Paris.**

Durée : 5 jours.

Tarif : Nous consulter

- Le coût de l'examen est **inclus** dans le tarif spécifique de cette formation,
- Les normes ISO/CEI 27001:2013, ISO/CEI 27002 : 2013, ISO/CEI 27003 : 2010 et ISO/CEI 27005 : 2011 de préparation à la certification Lead Implementer : ISO/CEI 27001 : 2013 ainsi que le Support de formation sont fournis au démarrage de la session de formation,
- Un certificat de participation de 35 CPE (Unités d'éducation continue / Continuing Professional Education) est remis aux participants en fin de formation.

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

PECB Certified Risk Manager ISO 27005 : 2011

[Réf : RMISO]

Cette formation a pour but de préparer les candidats à l'examen PECB Certified Risk Manager ISO/CEI 27005.

La formation intensive de trois jours propose les meilleures méthodes pour mener à bien un projet d'analyse de risque et à implémenter un programme de gestion des risques fondé sur la norme ISO/CEI 27005.

Tout au cours de la semaine, les participants sont invités à répondre à des questions, en groupe et individuellement, sur chacun des domaines et similaires à l'examen officiel.

Objectifs:

- Présenter les meilleures méthodes d'analyse de risques,
- Choisir une méthode adaptée à votre contexte,
- Enseigner la manière de conduire une analyse des risques de manière simplet et pragmatique.

Participants:

- Consultants et Spécialistes en Sécurité des Systèmes d'Information.

Pré-requis:

- Une connaissance préalable des normes ISO/CEI 27001 : 2013, ISO/CEI 27002 : 2013 et ISO/CEI 27005 : 2011 est recommandée,
- Une connaissance des techniques d'audit,
- La compréhension de l'anglais est nécessaire car une partie de la documentation fournie aux participants est en anglais.

Bénéfices attendus de la formation :

- Reconnaissance Internationale des compétences et des connaissances en analyse et gestion des risques conformément à la norme ISO/CEI 27005.

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

- Apporter d'une plus grande crédibilité dans la conduite de vos projets d'analyse de risque.

Intervenants :

- Les sessions sont animées par des Experts Seniors certifiés CISSP, CISSO, CISA, CISM, CBCP, CEH, CPEH, CPTE, Lead Auditor ISO 27001, Lead Implementer ISO 27001, Risk Manager ISO 27005, Risk Manager EBIOS, Risk Manager MEHARI.

Mode :

Formation inter – entreprises.

Programme:

Jour 1 : Concepts et définition du risque

- Concepts et définition du risque
- Le cadre normatif
- Mise en œuvre d'un programme de gestion du risque
- Etablissement du contexte

Jour 2 :

- Appréciation du risque
- Appréciation du risque avec une méthode quantitative
- Traitement du risque
- Acceptation du risque
- Communication relative aux risques
- Surveillance et réexamen des facteurs de risque
- Processus de certification Risk Manager ISO27005 et maintien

Jour 3 :

- Introduction à la méthode CRAMM
- Introduction à la méthode EBIOS
- Introduction à la méthode MEHARI
- Introduction à la méthode OCTAVE
- Introduction à la méthode Microsoft Security Risk Management
- Examen PECB Certified Risk Manager ISO/IEC 27005 :

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

L'examen PECB Certified Risk Manager ISO/CEI 27005 est disponible en français et dure 2 heures.
Le participant ayant réussi l'examen se verra délivrer une attestation de réussite. Pour réussir le participant devra obtenir un minimum de 70 points sur 100. Il sera qualifié de « Provisional Risk Manager » et disposera de 3 années pour demander à être certifié, « Risk Manager ISO/CEI 27005».

Lieu de formation et/ou d'examen :

- **Paris.**

Durée : 3 jours.

Tarif : Nous consulter.

- Le coût de l'examen est **inclus** dans le tarif spécifique de cette formation,
- La norme ISO/CEI 27005 : 2011 de préparation à la certification Risk Manager ISO/CEI 27005 ainsi que le Support de formation sont fournis au démarrage de la session de formation,
- Un certificat de participation de 21 CPE (Unités d'éducation continue / Continuing Professional Education) est remis aux participants en fin de formation.

Siege Social
2, rue du Colonel Dominé 75013 Paris

Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

PECB Certified Risk Manager : EBIOS

[Réf : RMEBI]

Objectifs :

La formation certifiante « PECB Certified Risk Manager EBIOS» traite de la gestion du risque de sécurité à travers la mise en œuvre de la méthode EBIOS de l'ANSSI. Cette formation vous permet de mener de bout en bout une appréciation des risques de l'étude des besoins à la formalisation des objectifs de sécurité.

En particulier, les objectifs de la formation sont les suivants :

- Appréhender la méthode EBIOS 2010 et ses différents cas d'utilisation.
- Donner les moyens au stagiaire de piloter et réaliser une appréciation des risques EBIOS.
- Communiquer les ressources et les outils disponibles afin de réaliser une appréciation des risques optimale.
- Préparer l'apprenant aux examens en fin de session.

Participants :

- La formation « PEDCB Certified Risk Manager EBIOS» s'adresse à toute personne souhaitant maîtriser la démarche EBIOS 2010 et/ou visant la certification Risk Manager EBIOS. Cette formation s'adresse à toute personne devant réaliser une appréciation des risques en sécurité, y comprit au delà des risques en sécurité informatique ;
- RSSI, chefs de projet SI et aux consultants en sécurité souhaitant maîtriser le processus de gestion des risques et EBIOS 2010.

Pré-requis :

- Posséder des connaissances de base en sécurité des systèmes d'information.

Bénéfices attendus de la formation :

- Acquérir les compétences pour implémenter et manager de façon continue un programme de management des risques de sécurité de l'information ;

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

- Acquérir les compétences pour conseiller efficacement les organisations sur les meilleures pratiques de management des risques de sécurité de l'information ;
- Comprendre les concepts, les approches, méthodes et techniques pour un management efficace des risques selon EBIOS ;
- Développer les compétences nécessaires pour conduire une appréciation de risque avec la méthode EBIOS ;
- Maîtriser les étapes pour conduire une appréciation des risques avec la méthode EBIOS
  Interpréter les exigences de la norme ISO 27001 relatives au management des risques de sécurité de l'information.

Intervenants :

- Les sessions sont animées par des Experts Seniors certifiés CISSP, CISSO, CISA, CISM, CBCP, CEH, CPEH, CPTE, Lead Auditor ISO 27001, Lead Implementer ISO 27001, Risk Manager ISO 27005, Risk Manager EBIOS, Risk Manager MEHARI.

Mode :

- Formation inter - entreprises.

Programme :

Jour 1 : Conduire une appréciation des risques avec EBIOS

- Présentation d'EBIOS
- Phase 1 – Etude du contexte
- Phase 2 – Etude des évènements redoutés
- Phase 3 – Etude des scénarios de menace

Jour 2 : Réaliser une appréciation des risques avec EBIOS

- Phase 4 - Etude de risque
- Phase 5 - Etude des mesures de sécurité
- Atelier avec étude de cas

Jour 3 : Examens PECB Certified Risk Manager EBIOS

- Examen de certification PECB Certified Risk Manager EBIOS (3 h) :
- L'examen de certification PECB Certified Risk Manager EBIOS couvre les domaines de compétences suivants :

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

- Domaine 1 : Principes fondamentaux et concepts dans la gestion des risques de sécurité de l'information basé sur EBIOS ;
- Domaine 2 : Programme de gestion des risques de sécurité de l'information basé sur EBIOS ;
- Domaine 3 : Appréciation des risques de sécurité de l'information basée sur EBIOS ;
- Domaine 4 : Traitement des risques de sécurité de l'information basé sur EBIOS ;
- Domaine 5 : Communication des risques de sécurité de l'information, surveillance et amélioration basées sur EBIOS.

Méthode :

- Ensemble d'exposés et d'exercices couvrant les parties du programme :
  - Exercices pratiques basés sur une étude de cas;
  - Tests pratiques similaires aux examens de certification Risk Manager EBIOS.

Lieu de formation :

- Paris.

Durée :

- 3 jours.

Tarif : Nous consulter

- Le Support de formation est fourni au démarrage de la session de formation ;
- Une copie du logiciel et de la documentation officielle EBIOS publiée par l'ANSSI est également fournie aux participants ;
- Un certificat de participation de 21 CPE (Unités d'éducation continue / Continuing Professional Education) est remis aux participants en fin de formation.

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

PECB Certified Risk Manager ISO 27005 avec EBIOS

[Réf : RMISE]

Objectifs :

La formation certifiante « PECB Certified Risk Manager ISO/CEI 27005:2011 avec la méthode EBIOS» traite de la gestion du risque de sécurité de l'information en général et de la méthode EBIOS de l'ANSSI. Cette formation vous permet de mener de bout en bout une appréciation des risques de l'étude des besoins à la formalisation des objectifs de sécurité.

En particulier, les objectifs de la formation sont les suivants :

- Maîtriser la construction d'un processus de gestion des risques selon la norme ISO/CEI 27005:2011 ;
- Appréhender la méthode EBIOS 2010 et ses différents cas d'utilisation.
- Donner les moyens au stagiaire de piloter et réaliser une appréciation des risques EBIOS.
- Communiquer les ressources et les outils disponibles afin de réaliser une appréciation des risques optimale.
- Préparer l'apprenant aux examens en fin de session.

Participants :

- La formation « PECB Certified Risk Manager ISO/CEI 27005:2011 avec la méthode EBIOS» s'adresse à toute personne souhaitant maîtriser la démarche EBIOS 2010 et/ou visant les certifications Risk Manager ISO27005:2011 et EBIOS Risk Manager. Cette formation s'adresse à toute personne devant réaliser une appréciation des risques en sécurité, y comprit au delà des risques en sécurité informatique ;
- RSSI, chefs de projet SI et aux consultants en sécurité souhaitant maîtriser le processus de gestion des risques et EBIOS 2010.

Pré-requis :

- Posséder des connaissances de base en sécurité des systèmes d'information.

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

Bénéfices attendus de la formation :

- Maîtriser le processus de management des risques selon la norme ISO/CEI 27005 :2011 ;
- Comprendre la relation entre le management des risques de sécurité de l'information, les mesures de sécurité et la conformité avec les exigences des différentes parties prenantes de l'organisation;
- Acquérir les compétences pour implémenter et manager de façon continue un programme de management des risques de sécurité de l'information ;
- Acquérir les compétences pour conseiller efficacement les organisations sur les meilleures pratiques de management des risques de sécurité de l'information ;
- Comprendre les concepts, les approches, méthodes et techniques pour un management efficace des risques selon EBIOS ;
- Développer les compétences nécessaires pour conduire une appréciation de risque avec la méthode EBIOS ;
- Maîtriser les étapes pour conduire une appréciation des risques avec la méthode EBIOS
  Interpréter les exigences de la norme ISO 27001 relatives aux management des risques de sécurité de l'information.

Intervenants :

- Les sessions sont animées par des Experts Seniors certifiés CISSP, CISSO, CISA, CISM, CBCP, CEH, CPEH, CPTE, Lead Auditor ISO 27001, Lead Implementer ISO 27001, Risk Manager ISO 27005, Risk Manager EBIOS, Risk Manager MEHARI.

Mode :

- Formation inter - entreprises.

Programme :

Jour 1 : Introduction, programme de gestion du risque, identification et analyse du risque selon ISO/CEI 27005

- Concepts et définitions liés à la gestion du risque,
- Normes, cadres de référence et méthodologies en gestion du risque,
- Mise en œuvre d'un programme de gestion du risque dans la sécurité de l´information,
- Analyse du risque (Identification et estimation).

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

Jour 2 : Evaluation du risque, traitement, acceptation, communication et surveillance selon ISO/CEI 27005

- Évaluation du risque,
- Traitement du risque,
- Acceptation du risque dans la sécurité de l´information et gestion du risque résiduel,
- Communication du risque dans la sécurité de l´information,
- Surveillance et contrôle du risque dans la sécurité de l´information,
- Examen Risk Manager ISO/CEI 27005 (durée : 2h). Couvre les domaines de compétences suivants :
    - Domaine 1 : Etude du contexte de l'organisation ;
    - Domaine 2 : Identification des actifs primaires et des actifs support ;
    - Domaine 3 : Identification des risques liés à la SSI ;
    - Domaine 4 : Traitement des risques liés à la SSI ;
    - Domaine 5 : Communication sur les risques liés à la SSI.

Jour 3 : Conduite d'une analyse de risques avec EBIOS

- Présentation EBIOS,
- Phase 1 – Etablissement du contexte,
- Phase 2 – Analyse des évènements redoutés de sécurité,
- Phase 3 – Analyse des scenarios de Menaces.

Jour 4 : Analyse de risques avec EBIOS

- Phase 4 - Analyse des risques,
- Phase 5 - Détermination des mesures de sécurité,
- Atelier avec des études de cas.

Jour 5 : Atelier avec des études de cas et Examen Risk Manager EBIOS

- Atelier avec des études de cas,
- Examen de certification PECB Certified Risk Manager EBIOS (Durée : 3 h). Couvre les domaines de compétence suivants :

    - Domaine 1 : Principes fondamentaux et concepts dans la gestion des risques de sécurité de l'information basé sur EBIOS ;
    - Domaine 2 : Programme de gestion des risques de sécurité de l'information basé sur EBIOS ;
    - Domaine 3 : Appréciation des risques de sécurité de l'information basée sur EBIOS ;
    - Domaine 4 : Traitement des risques de sécurité de l'information basé sur EBIOS ;

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

- Domaine 5 : Communication des risques de sécurité de l'information, surveillance et amélioration basées sur EBIOS.

Méthode :

- Ensemble d'exposés et d'exercices couvrant les parties du programme :
  - Exercices pratiques basés sur des études de cas;
  - Tests pratiques similaires aux examens de certification Risk manager ISO/CEI 27005 : 2011 et Risk Manager EBIOS.

Lieu de formation :

- **Paris.**

Durée :

- 5 jours.

Tarif : Nous consulter.

- Le Support de formation est fourni au démarrage de la session de formation ;
- Une copie de la norme ISO/CEI 27005 : 2011 est fournie aux participants ;
- Une copie du logiciel et de la documentation officielle EBIOS publiée par l'ANSSI est également fournie aux participants ;
- Un certificat de participation de 35 CPE (Unités d'éducation continue / Continuing Professional Education) est remis aux participants en fin de formation.

Siege Social
2, rue du Colonel Dominé 75013 Paris

Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

PECB Certified Risk Manager : MEHARI

[Réf : RMMEH]

Objectifs :

La formation certifiante « PECB Certified Risk Manager MEHARI» traite de la gestion du risque de sécurité à travers la mise en œuvre de la méthode MEHARI du CLUSIF. Cette formation vous permet de mener de bout en bout une appréciation des risques de l'étude des besoins à la formalisation des objectifs de sécurité.

En particulier, les objectifs de la formation sont les suivants :

- Appréhender la méthode MEHARI 2010 et ses différents cas d'utilisation.
- Donner les moyens au stagiaire de piloter et réaliser une appréciation des risques MEHARI.
- Communiquer les ressources et les outils disponibles afin de réaliser une appréciation des risques optimale.
- Préparer l'apprenant aux examens en fin de session.

Participants :

- La formation «PECB Certified Risk Manager MEHARI» s'adresse à toute personne souhaitant maîtriser la démarche MEHARI 2010 et/ou visant la certification Risk Manager MEHARI. Cette formation s'adresse à toute personne devant réaliser une appréciation des risques en sécurité, y comprit au delà des risques en sécurité informatique ;
- RSSI, chefs de projet SI et aux consultants en sécurité souhaitant maîtriser le processus de gestion des risques et MEHARI 2010.

Pré-requis :

- Posséder des connaissances de base en sécurité des systèmes d'information et de la méthode MEHARI est recommandée.

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

Bénéfices attendus de la formation :

- Acquérir les compétences pour implémenter et manager de façon continue un programme de management des risques de sécurité de l'information ;
- Acquérir les compétences pour conseiller efficacement les organisations sur les meilleures pratiques de management des risques de sécurité de l'information ;
- Comprendre les concepts, les approches, méthodes et techniques pour un management efficace des risques selon MEHARI ;
- Développer les compétences nécessaires pour conduire une appréciation de risque avec la méthode MEHARI ;
- Maîtriser les étapes pour conduire une appréciation des risques avec la méthode MEHARI
  Interpréter les exigences de la norme ISO/IEC 27001 relatives au management des risques de sécurité de l'information.

Intervenants :

- Les sessions sont animées par des Experts Seniors certifiés CISSP, CISSO, CISA, CISM, CBCP, CEH, CPEH, CPTE, Lead Auditor ISO 27001, Lead Implementer ISO 27001, Risk Manager ISO 27005, Risk Manager EBIOS, Risk Manager MEHARI.

Mode :

- Formation inter - entreprises.

Programme :

Jour 1 : Débuter une analyse de risque avec MEHARI

- Concepts et définitions reliés à la gestion du risque,
- Normes, cadres de référence et méthodologies en gestion du risque,
- Introduction à MEHARI,
- L'analyse des enjeux et la classification,
- L'échelle de valeur des dysfonctionnements,
- La classification des ressources.

Jour 2 : Analyse des vulnérabilités et du risque selon MEHARI

- L'analyse des vulnérabilités,
- Qualités d'un service de sécurité,
- Mesure de la qualité d'un service de sécurité,
- Processus d'évaluation,
- L'analyse des risques.

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

Jour 3 : Plan de sécurité selon MEHARI et Examen Risk Manager MEHARI

- Plans de sécurité et démarches,
- Outils d'aide à la mise en œuvre de MEHARI,
- Examen de certification PECB Certified Risk Manager MEHARI (Durée : 3 h).
    - Couvre les domaines de compétences suivants :
        - Domaine 1 : Principes fondamentaux et concepts dans la gestion des risques de sécurité de l'information basé sur MEHARI;
        - Domaine 2 : Programme de gestion des risques de sécurité de l'information basé sur MEHARI ;
        - Domaine 3 : Appréciation des risques de sécurité de l'information basée sur MEHARI ;
        - Domaine 4 : Traitement des risques de sécurité de l'information basé sur MEHARI ;
        - Domaine 5 : Communication des risques de sécurité de l'information, surveillance et amélioration basées sur MEHARI.

Méthode :

- Ensemble d'exposés et d'exercices couvrant les parties du programme :
    - Exercices pratiques basés sur une étude de cas;
    - Tests pratiques similaires aux examens de certification Risk Manager MEHARI.

Lieu de formation :

- **Paris.**

Durée :

- 3 jours.

Tarif : Nous consulter

- Le Support de formation est fourni au démarrage de la session de formation ;
- Une copie de la documentation officielle MEHARI publiée par le CLUSIF est également fournie aux participants ;
- Un certificat de participation de 21 CPE (Unités d'éducation continue / Continuing Professional Education) est remis aux participants en fin de formation.

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

PECB Certified Lead Cybersecurity Manager ISO 27032

[Réf : LCISO]

Cette formation a pour but de préparer les candidats à l'examen PECB Certified Lead Cybersecurity Manager ISO/IEC 27032.

Cette formation intensive de cinq jours permet aux participants de développer les compétences et les connaissances nécessaires pour assister une organisation dans la mise en oeuvre et la gestion d'un programme de cyber sécurité conforme à la norme ISO/IEC 27032 et au cadre de cyber sécurité NIST (Institut national américain des normes et de la technologie). Cette formation permet aux participants d'avoir un aperçu général de la cyber sécurité, de comprendre le lien entre la cyber sécurité et d'autres types de sécurité, et le rôle des différentes parties prenantes dans la cyber sécurité. Cette formation peut faire office de lignes directrices pour le traitement des questions courantes de cyber sécurité, et présente une structure qui permet aux parties prenantes de collaborer pour la résolution des problématiques de cyber sécurité.

Tout au cours de la semaine, les participants sont invités à répondre à des questions, en groupe et individuellement, sur chacun des domaines et similaires à l'examen officiel.

Objectifs:

- Maitriser les concepts fondamentaux, les principes, les approches, les normes, les méthodes et les techniques pour l'établissement et la gestion efficace d'un programme de cyber sécurité dans une organisation conformément à la norme ISO/IEC 27032.

Participants:

- Les professionnels en cyber sécurité ;
- Les experts de la sécurité de l'information ;
- Les responsables de projet souhaitant gérer un programme de cyber sécurité ;
- Les experts techniques souhaitant se préparer à occuper une fonction en cyber sécurité;
- Les personnes responsables du développement d'un programme de cyber sécurité.

Pré-requis:

Siege Social
2, rue du Colonel Dominé 75013 Paris

Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

- Une connaissance préalable des normes ISO/IEC 27001 : 2013, ISO/IEC 27002 : 2013 et ISO/IEC 27005 : 2011 est recommandée,

- La compréhension de l'anglais est nécessaire car la documentation fournie aux participants est en anglais.

Bénéfices attendus de la formation :

- Reconnaissance Internationale des compétences et des connaissances en analyse et gestion des risques de cyber sécurité conformément à la norme ISO/IEC 27032.
- Apporter d'une plus grande crédibilité dans la conduite de vos projets d'analyse de risque.

Intervenants :

- Les sessions sont animées par des Experts Seniors certifiés CISSP, CISSO, CISA, CISM, CBCP, CEH, CPEH, CPTE, Lead Auditor ISO 27001, Lead Implementer ISO 27001, Risk Manager ISO 27005, Risk Manager EBIOS, Risk Manager MEHARI.

Mode :

Formation inter – entreprises.

Programme:

Jour 1 : Introduction à la nome ISO/IEC 27032, initiation d'un programme de Cyber Sécurité

- Objectifs et structure de la formation
- Cadre normatif et réglementaire
- Concepts fondamentaux et définitions de la cyber sécurité
- Programme de cyber sécurité
- Initiation d'un programme de cyber sécurité
- Analyse de l'organisation
- Leadership

Jour 2 : Politique de cyber sécurité, gestion des risques et mécanismes d'attaque

- Politiques de cyber sécurité
- Gestion des risques en cyber sécurité
- Mécanismes d'attaque

Jour 3 : Mesures de cyber sécurité, coordination et partage de l'information

- Mesures de cyber sécurité
- Coordination et partage de l'information

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

- Programme de formation et de sensibilisation
-

Jour 4 : Gestion des incidents, surveillance et amélioration continue

- Continuité des activités
- Gestion des incidents de cyber sécurité
- Tests dans la cyber sécurité
- Mesure de la performance
- Réaction et récupération suite aux incidents de cyber sécurité
- Amélioration continue
- Schéma de certification Lead Manager
- Clôture de la formation

Jour 5 : Examen de certification

L'examen PECB Certified Lead Cybersecurity Manager ISO/IEC 27032 est disponible en anglais uniquement et dure 3 heures.

Il couvre les domaines de compétences suivants :

- Domaine 1 : Concepts fondamentaux ayant trait à la cyber sécurité ;
- Domaine 2 : Rôles et responsabilités des parties prenantes ;
- Domaine 3 : Gestion des risques en cyber sécurité ;
- Domaine 4 : Mécanismes d'attaque et mesures de cyber sécurité ;
- Domaine 5 : Partage de l'information et coordination ;
- Domaine 6 : Intégration d'un programme de cyber sécurité dans la gestion de la continuité des activités ;
- Domaine 7 : Gestion des incidents de cyber sécurité et mesure de la performance.

Le participant ayant réussi l'examen se verra délivrer une attestation de réussite. Pour réussir le participant devra obtenir un minimum de 70 points sur 100. Il sera qualifié de « Provisional Cybersecurity Manager ISO/IEC 27032 » et disposera de 3 années pour demander à être certifié « Cybersecurity Manager ISO/IEC 27032 » ou « Lead Cybersecurity Manager ISO/IEC 27032 ».

Lieu de formation et/ou d'examen :

- **Paris.**

Durée : 5 jours.

Tarif : Nous consulter.

- Le coût de l'examen est **inclus** dans le tarif spécifique de cette formation ;

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

- La norme ISO/IEC 27032 : 2012 de préparation à la certification Lead Cybersecurity Manager ISO/IEC 27032 ainsi que le support de formation sont fournis au démarrage de la session de formation ;
- Un certificat de participation de 35 CPE (Unités d'éducation continue / Continuing Professional Education) est remis aux participants en fin de formation.

Siege Social
2, rue du Colonel Dominé 75013 Paris

Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

PECB Certified Lead Implementer : ISO 22301 : 2012 (SMCA)

[Réf : LISMC]

Cette formation a pour but de préparer les candidats à l'examen PECB Certified Lead Implementer ISO/CEI 22301 : 2012, la certification internationale délivrée par PECB.

Cette formation propose aux participants une démarche méthodologique et les meilleures pratiques afin de leur permettre de développer l'expertise nécessaire pour aider une organisation dans la mise en œuvre et la gestion d'un Système de Management de la Continuité de l'Activité (SMCA) tel que spécifié dans l'ISO/CEI 22301 : 2012.

Tout au cours de la semaine, les participants sont invités à répondre à des questions, en groupe et individuellement, sur chacune des exigences de la norme et similaires à l'examen de certification officiel.

Objectifs :

- Acquérir les connaissances nécessaires à la réussite de l'examen Lead Implementer ISO/CEI 22301 : 2012 ,
- Maîtriser les exigences de la norme ISO/CEI 22301 :2012 et savoir l'implémenter dans le contexte d'une organisation ,
- Comprendre les besoins en continuité d'activité pour toute l'organisation ,
- Acquérir les connaissances nécessaires pour conseiller une organisation sur les meilleures pratiques en management de la continuité d'activité,
- Acquérir l'expertise nécessaire pour gérer une équipe de mise en œuvre d'un SMCA ISO/IEC 22301.

Participants :

- Chefs de projet ou consultants qui souhaitent préparer et assister une organisation dans la mise en œuvre de son Système de Management de la

Siege Social
2, rue du Colonel Dominé 75013 Paris

Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

Continuité des Activités (SMCA) - Auditeurs ISO/CEI 22301 qui souhaitent comprendre le processus de mise en œuvre d'un Système de Management de la Continuité des Activités - Les personnes responsables de la gestion de la continuité d'activité ou de la conformité dans une organisation - Membres d'une équipe en continuité des activités - Conseillers experts en continuité des activités - Experts techniques souhaitant se préparer à occuper une fonction en continuité des activités ou en gestion de projet SMCA.

Pré -requis :

- La compréhension de l'anglais est nécessaire car la documentation fournie aux participants est en anglais,
- Bonne connaissance des architectures du Système d'Information,
- Connaissance des concepts de base de Sécurité des Systèmes d'Information et de Continuité d'Activité.

Bénéfices attendus de la formation :

- Reconnaissance Internationale des compétences en Continuité d'Activité,
- Maîtriser les concepts fondamentaux de la Continuité d'Activité,
- Savoir dialoguer avec le management pour l'élaboration, l'implémentation et le maintien en condition opérationnelle d'un Système de Management de Continuité d'Activité (SMCA) conforme à la norme ISO/CEI 22301 :2012,
- Acquérir l'expertise nécessaire pour assister une organisation dans la mise en œuvre, la gestion et le maintien d'un SMCA, tel que spécifié dans ISO/CEI 22301 : 2012,
- Appréhender le rôle du Responsable Continuité dans l'organisation ,
- Gérer le management d'un projet SMCA.

Intervenants :

- Les sessions sont animées par des Experts Seniors certifiés CISSP, CISSO, CISA, CISM, CBCP, CEH, CPEH, CPTE, Lead Auditor ISO 27001, Lead Implementer ISO 27001, Risk Manager ISO 27005, Risk Manager EBIOS, Risk Manager MEHARI.

Mode :

Formation inter – entreprises.

Programme :

Le programme du séminaire suit les domaines définis pour l'examen :

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

Jour 1 : Introduction au concept de Système de Management de la Continuité des Activités (SMCA) tel que défini par l'ISO/CEI 22301 : 2012 ; Initialisation du SMCA :

- Introduction à la continuité d'activité,
- Introduction aux systèmes de management et à l'approche processus,
- Présentation des normes ISO 22301, ISO/PAS 22399 et ISO 27031, BS 25999, ainsi que le cadre réglementaire,
- Principes fondamentaux de la continuité de l'activité,
- Analyse préliminaire et détermination du niveau de maturité d'un système de management de continuité de l'activité existant d'après l'ISO 21827,
- Rédaction d'une étude de faisabilité et d'un plan projet pour la mise en œuvre d'un SMCA.

Jour 2 : **Planifier la mise en œuvre d'un SMCA basé sur l'ISO/CEI 22301 : 2012 :**

- Implémentation du SMCA – Phase PLAN (suite)
  - Mise en place d'une structure de gestion de la documentation,
  - Définition du périmètre du SMCA,
  - Définition de la politique et objectifs du SMCA,
  - Mise en place de la structure organisationnelle (Gouvernance de la continuité...) de la continuité de l'activité,
  - Analyse des impacts (BIA) et Appréciation des risques.

Jour 3 : **Mettre en place un SMCA basé sur l'ISO/CEI 22301 : 2012 :**

- Implémentation du SMCA – Phase DO
  - Mesures de protection et de mitigation :
    - Formalisation et mise des mesures de sécurité inscrites au Plan de Traitement des risques.
  - Elaboration d'un programme de sensibilisation et de formation à la continuité d'activité,
  - Elaboration d'une procédure d'audit interne,
  - Elaboration d'une procédure de gestion des incidents de sécurité,
  - Elaboration d'une procédure de Tableau de Bord (indicateurs de mesure d'efficacité et de conformité du SMCA),
  - Elaboration d'une procédure de revue de Direction du SMCA,
  - Détermination et évaluation des stratégies de continuité d'activité,
  - Développement des plans de continuité d'activité et rédaction des procédures,
  - Tests et exercices des plans de continuité d'activité.

Jour 4 : **Contrôler, surveiller, mesurer et améliorer un SMCA ; certification d'un SMCA :**

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

- Démarrage du SMCA – Phase CHECK
  - Surveillance et contrôle du SMCA :
    - Production des indicateurs du Tableau de Bord
  - Mis en œuvre du programme d'audit interne du SMCA,
  - Revue de direction du SMCA,
  - Préparation à l'audit de certification ISO/CEI 22301.
- Démarrage du SMCA – Phase ACT
  - Traitement des non-conformités,
  - Mise en œuvre d'un programme d'amélioration continue du SMCA.

Jour 5 : **Processus de certification PECB Certified ISO/CEI 22301 : 2012 et examen** :

- Processus de certification ;
- Examen de certification PECB Certified Lead Implementer ISO/CEI 22301 : 2012.

Examen et certification :

- L'examen écrit dure 3 heures et couvre les domaines de compétences suivants :
  - Domaine 1 : Principes et concepts fondamentaux de la continuité d'activité,
  - Domaine 2 : Code de bonnes pratiques de la continuité de l'activité basé sur l'ISO 22301,
  - Domaine 3 : Planifier un SMCA conforme à l'ISO/IEC 22301,
  - Domaine 4 : Mettre en œuvre un SMCA conforme à l'ISO/IEC 22301,
  - Domaine 5 : Évaluation de la performance, surveillance et mesure d'un SMCA conforme à l'ISO/IEC 22301,
  - Domaine 6 : Amélioration continue d'un SMCA conforme à l'ISO/IEC 22301,
  - Domaine 7 : Préparation de l'audit de certification d'un SMCA.

  Les résultats de l'examen vous parviendront par mail environ six à huit semaines plus tard. L'examen PECB Certified Lead Implementer ISO/CEI 22301 est disponible en français.
  Le participant ayant réussi l'examen se verra délivrer une attestation de réussite. Pour réussir le participant devra obtenir un minimum de 70 points sur 100. Il sera qualifié de « Provisional Implementer » et disposera de 3 années pour demander à être certifié, selon son niveau d'activité, « Implementer ISO/CEI 22301 » ou « Lead Implementer ISO/CEI 22301».

Lieu d'examen :

- **Paris.**

Durée : 5 jours.

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

Tarif : Nous consulter

- Le coût de l'examen est **inclus** dans le tarif spécifique de cette formation,
- Les normes ISO/CEI 22301:2012, ISO/CEI 17021 : 2011 de préparation à la certification Lead Implementer : ISO/CEI 22301 : 2012 ainsi que le Support de formation sont fournis au démarrage de la session de formation,
- Un certificat de participation de 35 CPE (Unités d'éducation continue / Continuing Professional Education) est remis aux participants en fin de formation.

Siege Social
2, rue du Colonel Dominé 75013 Paris

Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

CISM
(Certified Information Security Manager)

[Réf : CCISM]

Cette formation a pour but de préparer les candidats à l'examen du CISM (Certified Information Security Manager), la certification internationale délivrée par l'ISACA.

Attention :

- Cette formation n'est pas une formation au management de la sécurité,
- L'inscription à cette formation est totalement indépendante de celle à l'examen, qui se fait sur le site de l'ISACA (http://www.isaca.org).

Objectifs :

- Analyser les différents domaines du programme sur lequel porte l'examen,
- Assimiler le vocabulaire et les idées directrices de l'examen,
- S'entraîner au déroulement de l'épreuve et acquérir les stratégies de réponse au questionnaire.

Participants :

Ingénieurs Sécurité, RSSI, Consultants en Sécurité qui souhaitent obtenir la certification CISM (Certified Information Security Manager) délivrée par l'ISACA, et préparer l'examen. Celui-ci dure 4 heures et utilise un questionnaire constitué de 200 questions portant sur l'ensemble des domaines relevant du management de la sécurité du système d'information. Réussite à l'examen avec au moins un score de 450 points sur 800 (*).

Pré-requis :

- Expérience en matière de management de la sécurité des systèmes d'information,
- La compréhension de l'anglais est nécessaire car la documentation fournie aux participants est en anglais.

Bénéfices attendus de la formation :

- Reconnaissance Internationale des compétences en management de la sécurité des systèmes d'information,

Siege Social
2, rue du Colonel Dominé 75013 Paris

Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

- Savoir dialoguer avec le management pour la mise en oeuvre des mesures de sécurité pertinentes à l'atteinte des objectifs Business.
- Appréhender le rôle de RSSI dans l'organisation.

Intervenants :

- Les sessions sont animées par des Experts Seniors certifiés CISSP, CISSO, CISA, CISM, CBCP, CEH, CPEH, CPTE, Lead Auditor ISO 27001, Lead Implementer ISO 27001, Risk Manager ISO 27005, Risk Manager EBIOS, Risk Manager MEHARI.

Mode :

Formation inter – entreprises.

Programme :

Jour 1 :

- Domaine 1 : Gouvernance de la sécurité
- Domaine 2 : Management de la sécurité

Jour 2 :

- Domaine 3 : Gestion des plans de sécurité
- Domaine 4 : Gestion des activités de sécurité

Jour 3 :

- Domaine 5 : Gestion des incidents et réponses
- Simulation de l'examen

Méthode :

- Ensemble d'exposés couvrant chaque domaine du programme de l'examen.
- A la fin de chaque exposé, les participants doivent s'entraîner à répondre à un ensemble de questions portant sur le thème de l'exposé. Ces questions sont issues des précédentes sessions du CISM (ou d'examens comparables).

- Simulation partielle de l'examen (examen blanc) effectuée en fin de formation.

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

Lieu d'examen :

- Voir sur le site http://www.isaca.org

Durée : 3 jours.

Tarif : Nous consulter

- **Les frais d'examen ne sont pas compris dans le prix de cette session** ;
- Le Support de formation CISM est fourni au démarrage de la session de formation ;
- Un certificat de participation de 21 CPE (Unités d'éducation continue / Continuing Professional Education) est remis aux participants en fin de formation.

Siege Social
2, rue du Colonel Dominé 75013 Paris

Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

CISA
(Certified Information Systems Auditor)

[Réf : CCISA]

Cette formation a pour but de préparer les candidats à l'examen du CISA (Certified Information Systems Auditor), la certification internationale délivrée par l'ISACA, examen qui se déroule chaque année en juin et décembre.

Attention :

- Elle n'est en aucun cas une formation à l'audit du système d'information,
- L'inscription à cette formation est totalement indépendante de celle à l'examen qui doit se faire sur le site de l'ISACA (http://www.isaca.org).

Objectifs :

- Analyser les différents domaines du programme sur lequel porte l'examen,
- Assimiler le vocabulaire et les idées directrices de l'examen,
- S'entraîner au déroulement de l'épreuve et acquérir les stratégies de réponse au questionnaire.

Participants :

Auditeurs confirmés ou informaticiens (DSI, Ingénieurs, Experts Consultants) qui souhaitent obtenir la certification CISA (Certified Information Systems Auditor) délivrée par l'ISACA, et préparer l'examen. Celui-ci dure 4 heures et utilise un questionnaire constitué de 200 questions portant sur l'ensemble des domaines relevant de l'audit du système d'information. Réussite à l'examen avec au moins un score de 450 points sur 800 (*).

Pré – requis :

- Il est vivement recommandé aux auditeurs peu habitués à la problématique des réseaux et de la sécurité de suivre au préalable le séminaire ,
- La compréhension de l'anglais est nécessaire car la documentation fournie aux participants est en anglais.

Bénéfices attendus de la formation :

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

- Reconnaissance Internationale des compétences en audit des systèmes d'information,
- Savoir dialoguer avec le management pour la mise en oeuvre des mesures de sécurité pertinentes à l'atteinte des objectifs Business,
- Appréhender le rôle de l'Auditeur des SI dans l'organisation.

Intervenants :

- Les sessions sont animées par des Experts Seniors certifiés CISSP, CISSO, CISA, CISM, CBCP, CEH, CPEH, CPTE, Lead Implementer ISO 27001, Lead Auditor ISO 27001, Risk Manager ISO 27005, Risk Manager EBIOS, Risk Manager MEHARI.

Mode :

Formation inter – entreprises.

Programme :

Le programme du séminaire suit les 6 domaines définis pour l'examen :

Jour 1 :

- Domaine 1 : Processus d'audit des SI
  - Les standards d'audit,
  - L'analyse de risque et le contrôle interne,
  - La pratique d'un audit SI.
- Domaine 2 : Gouvernance des SI
  - Stratégie de la gouvernance du SI,
  - Procédures et Risk management,
  - La pratique de la gouvernance des SI,
  - L'audit d'une structure de gouvernance.

Jour 2 :

- Domaine 3 : Gestion du cycle de vie des systèmes et de l'infrastructure
  - Gestion de projet : pratique et audit,
  - Les pratiques de développement,
  - L'audit de la maintenance applicative et des systèmes,
  - Les contrôles applicatifs.

Jour 3 :

- Domaine 4 : Fourniture et support des services
  - Audit de l'exploitation des SI,
  - Audit des aspects matériels du SI,

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

- Audit des architectures SI et réseaux.

Jour 4 :

- Domaine 5 : Protection des avoirs informatiques
  - Gestion de la sécurité : politique et gouvernance,
  - Audit et sécurité logique et physique,
  - Audit de la sécurité des réseaux,
  - Audit des dispositifs nomades.

Jour 5 :

- Domaine 6 : Plan de continuité et plan de secours informatique
  - Les pratiques des plans de continuité et des plans de secours,
  - Audit des systèmes de continuité et de secours.

Dans chaque exposé, l'accent sera mis sur les éléments organisationnels et technologiques fondamentaux et leurs impacts sur la stratégie d'audit en termes de validité et d'exhaustivité des éléments audités conformément à l'approche ISACA.

Méthode :

- Un questionnaire d'auto-évaluation sur les différents domaines vous est proposé avant votre inscription à l'examen pour vous permettre d'évaluer éventuellement vos lacunes et y remédier en suivant une formation sur la sécurité, la sécurité des réseaux et Internet que vous propose **NL CONSULTING**,
- Ensemble d'exposés couvrant chaque domaine du programme de l'examen.
- A la fin de chaque exposé, les participants doivent s'entraîner à répondre à un ensemble de questions portant sur le thème de l'exposé. Ces questions sont issues des précédentes sessions du CISA (ou d'examens comparables).

- Simulation partielle de l'examen (examen blanc) effectuée en fin de formation.

Lieux d'examen :

- Voir sur le site http://www.isaca.org

Durée : 5 jours.

Tarif : Nous consulter

- **Les frais d'examen ne sont pas compris dans le prix de cette session** ;

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

- Le Support de formation est fourni au démarrage de la session de formation ;
- Un certificat de participation de 35 CPE (Unités d'éducation continue / Continuing Professional Education) est remis aux participants en fin de formation.

Siege Social
2, rue du Colonel Dominé 75013 Paris

Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

CPEH
(Certified Professional Ethical Hacker)

[Réf : CCPEH]

Cette formation certifiante a pour but de préparer les candidats à l'examen du **CPEH** (Certified Professional Ethical Hacker), la certification internationale délivrée par **MILE2**.

La formation CPEH constitue le cours de base de la ligne de cours « Test de pénétration » de MILE2. Elle s'appuie sur des d'exposés, des laboratoires permettant de mettre en oeuvre les meilleures pratiques de l'industrie en utilisant à la fois des outils open source et des outils commerciaux. Les laboratoires émulent des scénarios de piratage du monde réel et permettent au participant d'évaluer la sécurité de votre entreprise posture, l'aident à mettre en œuvre les mesure appropriées afin de mieux sécuriser l'infrastructure réseau, apprendre à combattre les pirates et / ou les virus, etc.

Tout au cours de la semaine, les participants sont aussi invités à répondre à des questions, en groupe et individuellement, sur chacun des domaines et similaires à l'examen officiel.

Attention :

- L'examen se fait sur le site de MILE2 (**http://www.mile2.com**) a lieu l'après-midi du 5e jour.

Objectifs :

- Acquérir les connaissances nécessaires à la réussite des examens CPEH ;
- Acquérir les connaissances et les compétences afin d'évaluer les vulnérabilités ;
- Acquérir les connaissances nécessaires pour conseiller une organisation sur les meilleures pratiques de sécurisation de l'IT.

Participants :

Responsable Informatique, Responsables de Sécurité, Ethical hackers, Pen Testers, Ingénieurs Sécurité, Auditeurs,… qui souhaitent obtenir la certification CPEH (Certified

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

Professional Ethical Hacker) délivrée par MILE2, et se présenter à l'examen à l'issue de la formation.

Pré -requis :

- Une expérience de douze mois dans le domaine des réseaux et de la sécurité ;
- La compréhension de l'anglais technique est nécessaire car le support de cours fourni aux participants est en anglais.

Bénéfices attendus de la formation :

- Reconnaissance Internationale des compétences en sécurité de l'information,
- Savoir dialoguer avec le management pour la mise en oeuvre des mesures de sécurité.

Intervenants :

- Les sessions sont animées par des Experts Seniors certifiés CISSP, CISSO, CISA, CISM, CBCP, CEH, CPEH, CPTE, Lead Auditor ISO 27001, Lead Implementer ISO 27001, Risk Manager ISO 27005, Risk Manager EBIOS, Risk Manager MEHARI.

Mode :

Formation inter – entreprises.

Programme :

Le programme de la formation suit les 14 domaines et les 5 annexes définis pour l'examen :

Jour 1 :

- Domaine 1 : Security Fundamentals
- Domaine 2 : Access Controls
- Domaine 3 : Protocols
- Domaine 4 : Cryptography

Jour 2 :

- Domaine 5 : Why Vulnerability Assessments ?
- Domaine 6 : Vulnerability Tools of the Trade
- Domaine 7 : Output Analysis and Reports

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

- Domaine 8 : Reconnaissance, Enumeration & Scanning

Jour 3 :

- Domaine 9 : Gaining Access
- Domaine 10 : Maintaining Access
- Domaine 11 : Covering Tracks
- Domaine 12 : Malware

Jour 4 :

- Domaine 13 : Buffer Overflows
- Domaine 14 : Passwords Cracking
- Appendix 1 : Economics and Laws
- Appendix 2 : Vulnerability Types

Jour 5 :

- Appendix 3 : Assessing Web Servers
- Appendix 4 : Assessing Remote & VPN services
- Appendix 5 : Denial of Services
- Examen de certification (après-midi)

- Examen de certification en ligne sur le site de MILE2 (durée 2 heures – 100 questions) ;
- Condition de réussite : au moins 700 points de bonnes réponses ;
- Résultat immédiat en fin d'examen avec envoi immédiat par e-mail du certificat CPEH en cas de réussite à l'examen.

Méthode :

- Ensemble d'exposés couvrant chaque domaine du programme de l'examen,
- A la fin de chaque exposé, les participants doivent s'entraîner à répondre à un ensemble de questions portant sur le thème de l'exposé. Ces questions sont issues des précédentes sessions du CPEH (ou d'examens comparables),
- Exercices réalisés en ligne tout au long de la formation sur le laboratoire virtuel de MILE2,
- Simulation partielle de l'examen (examen blanc) effectuée en fin de formation.

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

Lieu d'examen :

- Site http://www.mile2.com

Durée : 5 jours.

Tarif : Nous consulter

- **Les frais d'examen CPEH sont compris dans le prix de cette session**,
- Le support de formation CPEH en anglais est remis au démarrage de la session de formation,
- Un certificat de participation de 35 CPE (Unités d'éducation continue /Continuing Professional Education) est remis aux participants en fin de formation.

Siege Social
2, rue du Colonel Dominé 75013 Paris

Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

Maîtriser le processus d'élaboration d'une PSSI

[Réf : MPSSI]

Objectifs :

Au même titre que ses autres ressources (financières, physiques, humaines) l'information (stratégique, opérationnelle) est devenue une ressource importante pour toute organisation. La dépendance vis-à-vis du système d'information peut atteindre 85% dans les organisations de + 500 salariés. Par ailleurs, dans l'environnement actuel des organisations caractérisé par des interconnexions de plus en plus nombreuses, l'information est de plus en plus exposée et vulnérable. La sécurité du Système d'Information est devenue donc une préoccupation majeure. Dans ce contexte et étant donné l'importance des enjeux pour l'organisation, la complexité des processus, l'efficacité de la protection du système d'information ne peut être fondée sur une simple juxtaposition de mesures de sécurité « prêtes à l'emploi » mais sur une approche globale, exhaustive, systémique fondée sur l'étude de son contexte, la détermination de ses besoins de sécurité (métier, obligations réglementaires et légales), l'analyse des risques auxquels ses ressources sensibles sont exposés, l'identification de ses objectifs de sécurité et leur déclinaison en mesures de sécurité dont l'implémentation permettra d'éliminer les risques ou de les ramener à un niveau acceptable par l'organisation. L'ensemble des composants (enjeux, besoins de sécurité, menaces, règles de sécurité) de cette approche constitue la Politique de Sécurité du Système d'Information (PSSI). La sécurité de l'information et du système d'information devient un enjeu majeur et stratégique. C'est pourquoi, chaque organisme doit disposer d'une politique de sécurité du système d'information (PSSI).

En particulier, les objectifs de la formation sont les suivants :

- Sensibiliser à la nécessité de définir une PSSI adaptée aux objectifs stratégiques de l'organisation;
- Apprendre à élaborer et à mettre en place une PSSI de façon méthodique.

Participants :

- La formation « Maitriser le processus d'élaboration d'une PSSI» s'adresse à toute personne souhaitant maîtriser la démarche d'élaboration d'une Politique de Sécurité

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

des Systèmes d'Information : Directeurs Métiers, RSSI, chefs de projet SI et aux Consultants et Ingénieurs en Sécurité.

Pré-requis :

- Posséder des connaissances de base en sécurité des systèmes d'information.

Bénéfices attendus de la formation :

- Comprendre le rôle du document de définition de la politique de sécurité des systèmes d'informations (SSI), son périmètre global et sa nécessaire réactualisation ;
- Connaître les caractéristiques attendues d'un système d'information, en termes de sécurité ;
- Connaître l'existence de méthodes de mise en place d'une PSSI en incluant les règles de sécurité, à partir d'un modèle de référence ;
- Adapter ses comportements et ceux de son équipe en conformité avec la PSSI de l'établissement, dans son secteur d'activité particulier.

Intervenants :

- Les sessions sont animées par des Experts Seniors certifiés CISSP, CISSO, CISA, CISM, CBCP, CEH, CPEH, CPTE, Lead Auditor ISO 27001, Lead Implementer ISO 27001, Risk Manager ISO 27005, Risk Manager EBIOS, Risk Manager MEHARI.

Mode :

- Formation inter-entreprises.

Programme :

Jour 1 :

- **Partie 1 : Introduction**
  - Pourquoi une PSSI ?.
- **Partie 2 : Présentation et rôle de la PSSI**
  - Définitions et finalités de la PSSI;
  - Domaines d'application de la PSSI ;
  - Place de la PSSI dans le référentiel documentaire ;
  - Bases de légitimité de la PSSI.

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

- **Partie 3 : Démarche générale d'élaboration d'une PSSI**
    - Analyse de risque préalable.

Jour 2 :

- **Partie 3 : Démarche générale d'élaboration d'une PSSI (suite)**
  La méthode en 4 phases :
    - Phase 0 : Préalables ;
    - Phase 1 : Elaboration des éléments stratégiques;
    - Phase 2 : Sélection des principes et rédaction des règles ;
    - Phase 3 : Finalisation.

- **Partie 4 : Démarche générale d'élaboration d'une PSSI**
    - Norme ISO/IEC 27002 : 2013.

Jour 3 :

- **Partie 5 : Mise en application de la PSSI**
    - Introduction ;
    - Sensibilisation et communication ;
    - Adaptation comportementale ;

- **Partie 6 : Plan type et exemples de PSSI**
    - Plan type d'une PSSI
    - Exemples de PSSI

- **Partie 7 : Conclusion**

Méthode :

- Ensemble d'exposés et d'exercices couvrant les parties du programme :
    - Exercices pratiques basés sur une étude de cas.

Lieu de formation :

- **Paris.**

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

Durée :

- 3 jours.

Tarif : Nous consulter

- Le Support de formation est fourni au démarrage de la session de formation ;
- Une copie de la documentation officielle publiée par l'ANSSI est également fournie aux participants ;
- Un certificat de participation de 21 CPE (Unités d'éducation continue / Continuing Professional Education) est remis aux participants en fin de formation.

Siege Social
2, rue du Colonel Dominé 75013 Paris

Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

Maîtriser le processus d'élaboration d'un TdB SSI

[Réf : MTBSI]

Objectifs :

Contrôler sa sécurité est devenu indispensable afin de garantir que les investissements dans ce domaine sont à la mesure des enjeux.

En particulier, les objectifs de la formation sont les suivants :

- Sensibiliser à la nécessité de définir un Tableau d Bord SSI adapté aux objectifs SSI de l'organisation;
- Apprendre la construction d'indicateurs et de Tableaux de Bord SSI de façon méthodique pour une mise en œuvre efficace dans votre SI.

Participants :

- La formation « Maitriser le processus d'élaboration d'un Tableau de Bord SSI» s'adresse à toute personne souhaitant maîtriser la démarche d'élaboration d'un Tableau de Bord de Sécurité des Systèmes d'Information : Directeurs Métiers, RSSI, chefs de projet SI et aux Consultants et Ingénieurs en Sécurité.

Pré-requis :

- Posséder des connaissances de base en sécurité des systèmes d'information.

Bénéfices attendus de la formation :

- Comprendre le rôle du Tableau de Bord de Sécurité des systèmes d'informations (SSI)
- Connaître et maitriser l'approche de mise en place d'un Tableau de bord SSI ;
- Identifier les facteurs clé de succès pour mettre en place un tableau de bord ;
- Définir les indicateurs pertinents de son tableau de bord ;
- Mettre son Tableau de Bord en forme ;
- Utiliser le Tableau de Bord comme outil de pilotage et de management de la SSI.

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

Intervenants :

- Les sessions sont animées par des Experts Seniors certifiés CISSP, CISSO, CISA, CISM, CBCP, CEH, CPEH, CPTE, Lead Auditor ISO 27001, Lead Implementer ISO 27001, Risk Manager ISO 27005, Risk Manager EBIOS, Risk Manager MEHARI.

Mode :

- Formation inter– entreprises.

Programme :

Jour 1 :

- **Partie 1 : Introduction : contrôle de la sécurité**
- **Partie 2 : Indicateurs et instruments de mesure**
  - Définition
  - Type d'indicateurs
  - La tendance
  - Famille d'indicateurs
  - Représentation des indicateurs
  - Caractéristiques d'un bon indicateur
  - Conditions de réussite
  - Inscription dans une démarche ISO 27001 : 2013
  - Norme ISO 27004 : 2009 « Formation Security Management Measurement » : l'essentiel
- **Partie 3 : Méthode de détermination des indicateurs**
  - Définition
  - Définir du champ de mesure
  - Déterminer les objectifs
  - Identifier les critères
  - Etablir les paramètres de chaque critère
  - Composer l'indicateur

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

- Mode de fonctionnement
- Formaliser les indicateurs

Jour 2 :

- **Partie 4 : Tableaux de Bord**
  - Définition
  - A quoi sert-il ?
  - Les caractéristiques
  - Les types de tableaux de bord
  - La représentation
  - Conditions de réussite

- **Partie 5 : Démarche générale d'élaboration d'un Tableau de Bord SSI**
  - Introduction

  La démarche comporte 5 phases :

  - 1. Pré-requis ;
  - 2. Mis en place du projet « Tableau de Bord SSI » ;
  - 3. Elaboration des Tableaux de Bord SSI ;
  - 4. Exploitation des Tableaux de Bord SSI ;
  - 5. Evolution des Tableaux de Bord SSI ;

- **Partie 5 : Exemple d'application**
  - Etude de cas « Ministère » ;
  - Templates.

Méthode :

- Ensemble d'exposés et d'exercices couvrant les parties du programme :
  - Exercices pratiques basés sur une étude de cas.

Lieu de formation :

- **Paris.**

Durée :

- 2 jours.

Tarif : Nous consulter

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

- Le Support de formation est fourni au démarrage de la session de formation ;
- Une copie de la documentation officielle publiée par l'ANSSI est également fournie aux participants ;
- Un certificat de participation de 14 CPE (Unités d'éducation continue / Continuing Professional Education) est remis aux participants en fin de formation.

Siege Social
2, rue du Colonel Dominé 75013 Paris

Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

Cryptographie

[Réf : CRYPT]

Objectifs :

- Acquérir connaitre les différentes techniques cryptographiques et les principales applications ;
- Connaitre les chiffrements symétrique et asymétrique ;
- Connaitre le hachage, les algorithmes les plus utilisés et les méthodes de gestion des clés.

Participants :

- Ingénieurs et Informaticiens chevronnés.

Pré-requis :

- Connaissance des systèmes, réseaux et protocoles ;
- La compréhension de l'anglais est nécessaire.

Bénéfices attendus de la formation :

- Développer un expertise en ethical hacking et sécurité ;
- Développer son aptitude à proposer des recommandations pertinentes visant à réduire les risques dans le cadre de la conduite d'une mission de réalisation d'un test d'intrusion.

Intervenants :

- Les sessions sont animées par des Experts Seniors certifiés CISSP, CISSO, CISA, CISM, CBCP, CEH, CPEH, CPTE, Lead Auditor ISO 27001, Lead Implementer ISO 27001, Risk Manager ISO 27005, Risk Manager EBIOS, Risk Manager MEHARI.

Mode :

Formation inter - entreprises.

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr

Programme :

- Introduction
- Histoire des premiers documents chiffrés
- Services cryptographiques
- Concepts mathématiques
- Sécurité cryptographique et techniques d'attaque
- Chiffrement de flux (Stream Ciphers)
- Chiffrement par blocs (Block Ciphers)
- Chiffrement asymétrique
- Fonctions de hachage
- Intégrité et authentification
- Tierces Parties de confiance
- Standards divers

Méthode :

- Ensemble d'exposés et d'exercices couvrant les parties du programme.

Lieu de formation :

- Paris.

Durée : 5 jours.

Tarif : Nous consulter

- Le Support de formation est fourni au démarrage de la session de formation ;
- Un certificat de participation de 35 CPE (Unités d'éducation continue / Continuing Professional Education) est remis aux participants en fin de formation.

Siege Social
2, rue du Colonel Dominé 75013 Paris
Tél : +33 6 25 57 58 14
Email : nlabani@nl-consulting.fr