Présentation CONFISEC

Notre vision :

Conscient des enjeux et besoins à adresser dans le domaine de la cybersécurité, CONFISEC se positionne en tant que le référent et partenaire de confiance sur tous vos sujets liés à la cybersécurité et à la protection des données. Nous croyons que toute mission que vous nous confiez est le début d'un partenariat durable ou une opportunité de consolider celui-ci. Avec CONFISEC, nous voulons être dès vôtre.

Notre métier :

CONFISEC est une firme spécialisée en services et prestations en matière de cybersécurité et de protection des données. Nos collaborateurs sont à la base des consultants formés en cybersécurité et protection des données. Nous mettons à votre disposition en fonction du sujet des :

- Directeurs de projet/programme en cybersécurité
- Chefs de projet cybersécurité
- Auditeurs / consultants cybersécurité
- Assistants RSSI
- Intégrateurs de solutions cybersécurité

Nos atouts

- Une connaissance du contexte africain et des enjeux règlementaires liés à la cybersécurité;
- Une société de services professionnels axés sur la compétence, avec une compréhension des défis, des tendances et des pratiques en matière de sécurité;
- Une société au service des organisations publiques, des PME et des grandes entreprises;
- Un très large éventail de services et d'offres en matière de cybersécurité afin d'accompagner vos projets SI et numériques;
- Une équipe de professionnels, jeunes et passionnés, dotés de « Soft Skills » et capable de s'adapter à votre environnement;
- Une réputation d'excellence sur le marché.

Nos services

Audits & Evaluation	**Conseil**
Sécurité des technologies	**Formations et sensibilisation**
RSSI « as a service »	**Cybersécurité régalienne**

La formation en cybersécurité,

Un incontournable pour édifier votre protection contre les cybermenaces

Le saviez-vous ?

Toutes les normes ISO renferment une clause intitulée « Compétences » évoquant la nécessité de confier la gestion des systèmes de management à des personnes compétentes sur la base d'une formation initiales ou continue.

Les technologies ne peuvent à elles seules suffire même si elles sont aussi indispensables pour protéger vos données. La sécurité de vos données reposera toujours sur les aptitudes des ingénieurs à gérer efficacement les différentes mesures de sécurité tant sur le plan technique qu'organisationnel. Seule la formation initiale et même continue garantira la mise à niveau ou la mise à jour des connaissances et compétences en matière de sécurité des données.

3,5 millions ! C'est le nombre de postes en cybersécurité non pourvus en 2021. Et ce chiffre ne fera que grimper dans les années à venir

Ceci témoigne des défis colossaux que font face aux différentes organisations pour trouver les profils spécialisés dans ce domaine. Quand on ne peut trouver la perle rare, il est donc possible pour chaque entreprise d'investir dans la formation cybersécurité de ses ressources, ce qui au-delà des besoins internes peut s'avérer motivant pour les collaborateurs dans leur plan de carrière.

Toutes les études sérieuses en matière de gestion des ressources humaines projettent les métiers liés à la cybersécurité parmi les métiers du futur.

Ce n'est donc pas étonnant d'observer de plus en plus des reconversions professionnelles vers ces métiers qui deviennent une aubaine pour le développement des carrières.

Ces constats nous montrent qu'il existe aujourd'hui des enjeux majeurs d'adaptation des compétences, auxquels seule la formation professionnelle initiale et/ou continue peut répondre.

Adaptation, mais aussi individualisation et qualification… C'est tout l'esprit de notre catalogue de formation.

Nous sommes convaincus que ce catalogue répondra à vos attentes et restons disponibles pour tout besoin spécifique en matière de formation sur la sécurité des données.

La Direction Générale CONFISEC

Citations

« Nous sommes ce que nous faisons de manière répétitive, l'excellence n'est donc pas un acte mais une habitude » Aristote

« Investir dans la formation c'est conjuguer au présent mais aussi au futur le souci des hommes et le souci des résultats. » Philippe BLOCH

Typologies de formation

Formation inter-entreprises

- Une formation inter-entreprises réunit des collaborateurs de plusieurs organismes
- Les formations ont lieu dans les locaux de CONFISEC ou dans un autre endroit choisi par CONFISEC.
- CONFISEC fixe les dates
- Pour ce genre de formation, le tarif par participant est public et fixe
- Vous bénéficiez d'un partage d'expérience entre collaborateurs venant d'organismes et de secteurs d'activités différents. Les méthodes de travail ne sont pas les mêmes partout et certaines bonnes pratiques sont facilement échangées pendant les sessions
- Toute la logistique est à la charge de CONFISEC

Formation intra-entreprise

- La plupart des formations du catalogue peuvent être dispensées en intra-entreprise, uniquement avec des collaborateurs de votre organisme, dans vos locaux.
- Si vous avez un besoin spécifique de formation qui ne se trouve pas dans notre catalogue, nous pouvons concevoir une formation sur mesure, spécifique à votre contexte
- La formation ne rassemble que les collaborateurs de votre organisme
- La formation permet d'aborder des problématiques internes et de poser des questions propres à votre organisation
- La formation peut se dérouler dans les locaux de CONFISEC si vous ne disposez pas de moyens logistiques adéquats
- La session de formation est planifiable selon les disponibilités des participants et au moment de votre choix

Coaching personnalisé

- Une formation sur mesure selon vos besoins et vos choix de modules
- Un plan d'actions défini avec nos consultants formateurs
- Un entretien individuel de suivi après chaque module ; permettant ainsi de vérifier s'il y a des difficultés lors de la mise en application du plan d'actions

Nos engagements qualité :

CONFISEC s'engage à :

- Faire intervenir des formateurs certifiés dans le domaine de la formation dispensée et ayant une expérience terrain
- Fournir des supports de formation de qualité lors des sessions organisées

- Être à l'écoute à travers les évaluations à chaud et à froid des sessions de formations et des formateurs
- Se conformer aux conditions générales de vente
- Traiter dans la mesure du possible aux dysfonctionnements qui peuvent impacter la qualité de la formation
- Limiter le nombre de participants à un maximum de 10 participants par session afin d'allouer un temps conséquent du formateur aux participants

A qui s'adresse nos formations ?

Public cible	**Plus-value des formations dispensées**
Dirigeants d'entreprises	○ Meilleure connaissance des enjeux sécurité ○ Aide à l'orientation sur les choix en matière de sécurité de l'information ○ Meilleure assimilation du cadre règlementaire applicable
RSSI & équipe en charge de la cybersécurité	○ Renforcement des compétences ○ Capacité d'apprendre des pairs ○ Retour d'expérience terrain des formateurs
DPO & équipe en charge de la protection des données personnelles	○ Renforcement des compétences ○ Approfondissement des connaissances sur la protection des données ○ Retour d'expérience terrain des formateurs
Informaticiens	○ Renforcement de la sensibilisation sur la cybersécurité ○ Renforcement des aptitudes à protéger le système d'information
Auditeurs & fonctions de contrôle interne	○ Renforcement de la capacité à auditer selon des référentiels spécialisés en sécurité ○ Meilleure assimilation des risques liés à la sécurité de l'information

Nos formateurs

CONFISEC dispose d'une équipe de formateurs hautement qualifiés. La plupart de ses consultants ont acquis une expérience à l'international et sont dotés de certifications internationalement reconnues dans le domaine de la sécurité. Il s'agit notamment des certifications suivantes :

CISSP, ISO 27001 Master, ISO 27032 Lead Cybersecurity Manager, Data Protection Officer, ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, CEH, OSCP, CISM…

Niveaux de formation

Cursus	○ Parcours de formations dans le cadre d'un programme combiné lié à un métier ○ Codification : CURS
Sensibilisation	○ Initiation ou Perfectionnement aux concepts généraux de la cybersécurité ○ Format court n'excédant pas 1 jour ○ Codification : SENS
Fondamentaux	○ Introduction aux concepts généraux et sur les domaines tels que la gestion des risques, la réglementation, le management de la cybersécurité, la continuité d'activités. Ces modules s'adressent à des publics larges. ○ Codification : FOND
Compétences générales	○ Notions avancées et état de l'art en techniques de protection, dans la gestion de la sécurité des données, etc … ○ Accents mis sur les études de cas ○ Ces modules s'adressent à un public davantage ciblé devant mettre en pratique au quotidien son savoir et son expertise en sécurité des données ○ Codification : GEN
Compétences pointues	○ Formations poussées en particulier sous forme de travaux pratiques sur des disciplines d'expertise en cybersécurité : audit technique et tests d'intrusion, usage des méthodes de gestion des risques, sécurité des technologies, … ○ Ces modules s'adressent à des professionnels de la cybersécurité ○ Codification : POINT

Sommaire des formations

Titre formation	Nbr de jours	Profil des candidats	Certifiante ?
Sécurité de l'information			
ISO 27001 Foundation	2	Managers	Oui

ISO 27001 Lead Implementer	5	Managers en sécurité de l'information	Oui
ISO 27001 Lead Auditor	5	Auditeurs	Oui
ISO 27002 Manager	3	Gestionnaires de mesures de sécurité de l'information Contrôleurs internes	Oui
ISO 27002 Lead Manager	5	Gestionnaires de mesures de sécurité de l'information	Oui
ISO 27005 Risk Manager	3	Gestionnaires des risques Contrôleurs internes	Oui
EBIOS Risk Manager	3	Membres d'une équipe de gestion des risques sécurité SI	Oui
MEHARI Risk Manager	3	Membres d'une équipe de gestion des risques sécurité SI	Oui
	Cybersécurité		
Cybersécurité en entreprise	1	Directeurs	Non
ISO 27032 Lead Cybersecurity Manager	5	Membres d'une équipe de gestion de la cybersécurité	Oui
Lead Pen Test Professionnel	5	Membres d'une équipe de gestion de la cybersécurité	Oui
	Continuité d'activité		
ISO 22301 Foundation	2	Managers	Oui
ISO 22301 Lead Implementer	5	Managers de la continuité d'activité	Oui
ISO 22301 Lead Auditor	5	Auditeurs	Oui
	Protection des données personnelles		
RGPD Foundation	2	Managers	Oui
Data Protection Officer	5	Membre d'une équipe de gestion de la conformité	Oui
	Bloc de compétences		
Métier RSSI	13	RSSI ou Aspirants RSSI	Oui
Auditeur sécurité SI	13	Auditeurs ou Aspirants auditeurs sécurité SI	Oui
	Sécurité des technologies		
Etat de l'art	3	Membres d'une entité en charge des systèmes d'information	Non
Sécurité Windows	3	Administrateurs système	Non

Programme des formations

ISO 27001 Foundation

Durée : 2 jours

Objectifs :

- Comprendre la mise en œuvre d'un Système de Management de la Sécurité de l'Information (SMSI) conforme à l'ISO 27001.
- Comprendre la relation entre un SMSI (incluant le management des risques et des contrôles) et la conformité aux exigences des déférentes parties prenantes d'une organisation.
- Acquérir les connaissances nécessaires pour contribuer à la mise en œuvre d'un SMSI tel que spécifié dans la norme ISO 27001

Audience :

- Manager.
- Professionnel IT.
- RSSI.
- Auditeur SI.

Prérequis : Aucun

Contenu de la formation :

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

- Introduction à la famille des normes ISO 27000.
- Introduction aux systèmes de management et à l'approche processus.
- Principes fondamentaux en sécurité de l'information.
- Exigences générales : présentation des clauses 4 à 10 de la norme ISO 27001
- Phases de mise en œuvre du cadre ISO 27001.
- Amélioration continue de la Sécurité de l'Information.
- Conduire un audit de certification ISO 27001

2- Mettre en œuvre des mesures de sécurité de l'information conformes à l'ISO 27002 et examen de certification

- Principes et élaboration de mesures de sécurité de l'information.
- Documentation d'un environnement de contrôle de sécurité de l'information.
- Contrôle et surveillance des mesures de sécurité de l'information
- Exemples de mise en œuvre de mesures de sécurité de l'information basées sur les meilleures pratiques de l'ISO 27002.
- Examen Certified ISO/IEC 27001 Foundation.

ISO 27001 Lead Auditor

Durée : 5 jours

Objectifs :

- Comprendre la relation entre le système de management de la sécurité de l'information, le management des risques et les mesures.

- Comprendre les principes, procédures et techniques d'audit de la norme ISO 19011 :2018, et comment les appliquer dans le cadre d'un audit selon la norme ISO 27001.
- Acquérir les compétences nécessaires pour auditer un SMSI conformément aux exigences de l'ISO 27001, et les techniques de gestion d'une équipe d'audit.
- Préparer et compléter un rapport d'audit ISO 27001

Audience :

- Auditeur interne
- Equipe de contrôle interne
- Personne désirant diriger des audits de certification ISO 27001 en tant que responsable d'une équipe d'audit
- Consultant désirant préparer et accompagner une organisation lors d'un audit de certification ISO 27001

Prérequis : Une connaissance préalable des normes ISO 27001 et ISO 27002 est recommandée

Contenu de la formation :

1- Introduction à la gestion d'un système de management de la sécurité de l'information selon ISO 27001

- Cadre normatif et réglementaire
- Processus de certification ISO 27001
- Principes fondamentaux de la sécurité de l'information et de la gestion des risques
- Système de management de la sécurité de l'information (SMSI).
- Présentation des clauses 4 à 10 de la norme ISO 27001

2- Démarrer un audit ISO 27001

- Concepts et principes fondamentaux d'audit
- Éthique et déontologie d'audit
- L'approche d'audit fondée sur la preuve et sur le risque
- Préparation d'un audit de certification ISO 27001
- L'audit documentaire
- Préparation du plan d'audit.
- Conduite d'une réunion d'ouverture.

3- Conduire un audit ISO 27001

- Communication durant l'audit
- Les procédures d'audit (observation, entrevue, techniques d'échantillonnage).
- Rédaction des conclusions d'audit et des rapports de non-conformité

4- Conclure un audit ISO 27001

- Documentation d'audit
- Revue des notes d'audit
- Conclusion d'un audit ISO 27001
- Gestion d'un programme d'audit
- La compétence et l'évaluation des auditeurs.
- Clôture de l'audit.

5- Examen

ISO 27001 Lead Implementer

Durée : 5 jours

Objectifs :

- 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

Audience :

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

Prérequis : Une connaissance préalable des normes ISO 27001 et ISO 27002 est recommandée

Contenu de la formation :

1- Introduction à ISO/IEC 27001 et initiation d'un SMSI

- Objectifs et structure de la formation
- Normes et cadres réglementaires
- Système de management de la sécurité de l'information (SMSI)
- Concepts et principes fondamentaux de la sécurité de l'information
- Initiation de la mise en œuvre du SMSI
- Compréhension de l'organisme et de son contexte
- Périmètre du SMSI

2- Planification de la mise en œuvre d'un SMSI

- Concepts et principes fondamentaux d'audit
- Leadership et approbation du projet
- Structure organisationnelle h Analyse du système existant
- Politique de sécurité de l'information
- Gestion des risques
- Déclaration d'applicabilité

3- Mise en œuvre d'un SMSI

- Gestion de l'information documentée
- Sélection et conception des mesures de sécurité
- Mise en œuvre des mesures de sécurité
- Tendances et technologies
- Communication
- Compétence et sensibilisation
- Gestion des opérations de sécurité

4- Surveillance du SMSI, amélioration continue et préparation à l'audit de certification

- Surveillance, mesure, analyse et évaluation
- Audit interne
- Revue de direction

- Traitement des non-conformités
- Amélioration continue
- Préparation à l'audit de certification
- Processus de certification et clôture de la formation

5- Examen

ISO 27002 Manager

Durée : 3 jours

Objectifs :

- Comprendre la corrélation entre la norme ISO/CEI 27002 et la norme ISO/CEI 27001
- Comprendre la mise en œuvre des mesures de sécurité d'information en conformité avec la norme ISO /CEI 27002
- Développer l'expertise pour soutenir une organisation dans la mise en œuvre, la gestion et le maintien des mesures de sécurité d'information
- Comprendre la formulation et la mise en œuvre des exigences et des objectifs de la sécurité d'information

Audience :

- Responsables désirant mettre en œuvre un système de la sécurité d'information (SMSI) conforme aux normes ISO/CEI 27001 et ISO/CEI 27002
- Tout individu responsable de la sécurité d'information dans une organisation
- Membres de l'équipe de sécurité de l'information
- Conseillers spécialisés en technologies de l'information
- Professionnels des TI
- Agents de la protection des données personnelles
- Agents de la sécurité de l'information

Prérequis : Des connaissances fondamentales de la norme ISO/CEI 27002 et des connaissances approfondies sur la sécurité de l'information.

Contenu de la formation :

1- Introduction aux mesures de sécurité d'information selon la norme ISO/CEI 27002

- Objectifs et structure de la formation
- Cadres normatifs et réglementaires
- Principes fondamentaux de la sécurité de l'information
- Système de mangement de la sécurité de l'information
- Politiques de sécurité de l'information
- Management de la sécurité de l'information
- Sécurité des ressources humaines

2- Exigences et objectifs de la sécurité de l'information conformes à la norme ISO/CEI 27002

- Gestion des actifs
- Contrôle d'accès
- Cryptographie
- Sécurité physique et environnementale
- Sécurité liée à l'exploitation

3- Exigences et objectifs de la sécurité de l'information conformes à la norme ISO/CEI 27002 (suite et fin)

- Sécurité des communications

- Acquisition, développement et maintenance des systèmes d'information
- Relations avec les fournisseurs
- Gestion des incidents liés à la sécurité de l'information
- Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité
- Conformité
- Compétences et évaluation des gestionnaires
- **Examen**

ISO 27002 Lead Manager

Durée : 5 jours

Objectifs :

- Maîtriser la mise en œuvre des mesures de sécurité de l'information en respectant le cadre et les principes de la norme ISO/CEI 27002
- Maîtriser les concepts, les approches, les normes et les techniques nécessaires pour la mise en œuvre et la gestion efficace des mesures de la sécurité d'information
- Comprendre la relation entre les différentes composantes des mesures de sécurité de l'information, y compris la responsabilité, la stratégie, l'acquisition, la performance, la conformité et le comportement humain
- Comprendre l'importance de la sécurité d'information pour la stratégie de l'organisation
- Maîtriser la mise en œuvre des processus de la sécurité d'information
- Maîtriser l'expertise pour soutenir une organisation dans la mise en œuvre, la gestion et le maintien des mesures de la sécurité de l'information
- Maîtriser la formulation et la mise en œuvre des exigences et des objectifs de la sécurité d'information

Audience :

- Responsables désirant mettre en œuvre un système de la sécurité d'information (SMSI) conforme aux normes ISO/CEI 27001 et ISO/CEI 27002
- Tout individu responsable de la sécurité d'information dans une organisation
- Membres de l'équipe de sécurité de l'information
- Conseillers spécialisés en technologies de l'information
- Professionnels des TI
- Agents de la protection des données personnelles
- Agents de la sécurité de l'information

Prérequis : Des connaissances fondamentales de la norme ISO/CEI 27002 et des connaissances approfondies sur la sécurité de l'information.

Contenu de la formation :

1- Introduction aux mesures de sécurité d'information selon la norme ISO/CEI 27002

- Objectifs et structure de la formation
- Cadres normatifs et réglementaires
- Principes fondamentaux de la sécurité de l'information
- Système de mangement de la sécurité de l'information
- Politiques de sécurité de l'information
- Management de la sécurité de l'information
- Sécurité des ressources humaines

2- Exigences et objectifs de la sécurité de l'information conformes à la norme ISO/CEI 27002

- Sécurité des ressources humaines
- Gestion des actifs
- Contrôle d'accès

3- Exigences et objectifs de la sécurité de l'information conformes à la norme ISO/CEI 27002

- Cryptographie
- Sécurité des communications
- Sécurité physique et environnementale
- Sécurité liée à l'exploitation

4- Exigences et objectifs de la sécurité de l'information conformes à la norme ISO/CEI 27002

- Acquisition, développement et maintenance des systèmes d'information
- Relations avec les fournisseurs
- Gestion des incidents liés à la sécurité de l'information
- Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité
- Conformité
- Compétences et évaluation des gestionnaires

5- Examen

ISO 27005 Risk Manager

Durée : 3 jours

Objectifs :

- Acquérir l'expertise nécessaire pour gérer de façon responsable un processus de gestion des risques liés à la sécurité de l'information
- Acquérir une connaissance approfondie des spécificités de la gestion des risques de sécurité de l'information dans le cadre d'un programme de gestion globale des risques d'entreprise
- Obtenir les compétences nécessaires pour accompagner la mise en œuvre efficace d'un processus de gestion des risques liés à la sécurité de l'information au sein d'une organisation

Audience :

- Responsables de la sécurité d'information
- Membres d'une équipe de sécurité de l'information
- Tout individu responsable de la sécurité d'information, de la conformité et du risque dans une organisation
- Tout individu mettant en œuvre ISO/IEC 27001, désirant se conformer à la norme ISO/IEC 27001 ou impliqué dans un programme de gestion des risques
- Consultants des TI
- Professionnels des TI
- Agents de la protection des données personnelles
- Auditeurs TI désirant rehausser ses connaissances dans le domaine de la gestion des risques de sécurité de l'information

Prérequis : Des connaissances fondamentales dans la gestion des risques en entreprise

Contenu de la formation :

1- Introduction au programme de gestion des risques conforme à ISO/IEC 27005

- Objectifs et structure de la formation
- Cadres normatifs et règlementaires
- Concepts et définitions du risque
- Programme de gestion des risques

- Établissement du contexte

2- Mise en œuvre d'un processus de gestion des risques conforme à ISO/IEC 27005
- Identification des risques
- Analyse et évaluation des risques
- Appréciation du risque avec une méthode quantitative
- Traitement des risques
- Acceptation des risques et gestion des risques résiduels
- Communication relative aux risques
- Surveillance et réexamen des risques

3- Aperçu des autres méthodes d'appréciation des risques liés à la sécurité de l'information et examen de certification
- Méthode OCTAVE
- Méthode MEHARI
- Méthode EBIOS
- Méthodologie harmonisée d'EMR
- Examen

MEHARI Risk Manager

Durée : 3 jours

Objectifs :
- Comprendre et découvrir la puissance de la méthode MEHARI
- Cartographier les risques avec la méthode MEHARI
- Maîtriser les éléments de gestion des risques de base pour la sécurité de l'information, en utilisant la méthode MEHARI
- Pratiquer la gestion des risques avec la méthode MEHARI
- Analyser et communiquer les résultats d'une étude MEHARI

Audience :
- Personnes souhaitant apprendre les concepts fondamentaux du management des risques
- Personnes participant aux activités d'appréciation des risques sur les SI
- Responsables désirant comprendre les techniques d'appréciation des risques basées sur la méthode MEHARI
- Responsables souhaitant maîtriser les techniques d'analyse et de communication des résultats d'appréciation des risques selon la méthode MEHARI

Prérequis : Des connaissances fondamentales dans la gestion des risques en entreprise

Contenu de la formation :

1- Introduction aux concepts et aux étapes de la méthode d'analyse de risque MEHARI

2- Conduire une analyse de risque en utilisant la méthode MEHARI

3- Planification de la sécurité selon la méthode MEHARI et examen de certification

ISO 27032 Lead Cybersecurity Manager

Durée : 5 jours

Objectifs :

- Acquérir des connaissances approfondies sur les composantes et les opérations d'un programme de cybersécurité en conformité avec l'ISO/IEC 27032 et le cadre de cybersécurité NIST
- Comprendre la corrélation entre ISO 27032, le cadre de cybersécurité NIST et les autres normes et cadres réglementaires
- Maîtriser les concepts, approches, normes, méthodes et techniques pour établir, mettre en œuvre et gérer efficacement un programme de cybersécurité au sein d'un organisme
- Apprendre à interpréter les exigences d'ISO/IEC 27032 dans le contexte spécifique d'un organisme
- Maîtriser l'expertise nécessaire pour planifier, mettre en œuvre, gérer, contrôler et maintenir un programme de cybersécurité tel que spécifié dans ISO/IEC 27032 et le cadre de cybersécurité NIST
- Acquérir les compétences pour conseiller un organisme sur les bonnes pratiques de management de la cybersécurité

Audience :

- Professionnels de la cybersécurité
- Experts en sécurité de l'information
- Professionnels souhaitant gérer un programme de cybersécurité
- Responsables du développement d'un programme de cybersécurité
- Spécialistes des TI
- Conseillers spécialisés dans les TI
- Professionnels des TI souhaitant accroître leurs connaissances et compétences techniques

Prérequis : Des connaissances fondamentales de la norme ISO/CEI 27002 et des connaissances approfondies sur la sécurité de l'information.

Contenu de la formation :

1- Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032

- Normes et cadres réglementaires
- Notions fondamentales de la cybersécurité
- Programme de cybersécurité
- Lancer un programme de cybersécurité
- Analyser l'organisme
- Leadership

2- Politiques de cybersécurité, management du risque et mécanismes d'attaque

- Politiques de cybersécurité
- Gestion du risque de la cybersécurité
- Mécanismes d'attaque

3- Mesures de contrôle de cybersécurité, partage et coordination de l'information

- Mesures de contrôle de cybersécurité
- Partage et coordination de l'information
- Programme de formation et de sensibilisation

4- Gestion des incidents, suivi et amélioration continue

- Continuité des activités
- Management des incidents de cybersécurité

- Intervention et récupération en cas d'incident de cybersécurité
- Conclusion de la formation
- Tests en cybersécurité
- Mesure de la performance
- Amélioration continue

5- Examen

Lead Pen Test Professionnel

Durée : 5 jours

Objectifs :

- Savoir interpréter et illustrer les principaux concepts et principes relatifs au test d'intrusion
- Comprendre les connaissances techniques de base nécessaires pour organiser et mener à bien un ensemble efficace de tests d'intrusion
- Apprendre comment planifier efficacement un test d'intrusion et identifier un domaine d'application approprié et adapté en fonction du risque
- Acquérir les connaissances et les compétences pratiques sur les outils et les techniques utilisés pour effectuer efficacement un test d'intrusion
- Gérer efficacement le temps et les ressources nécessaires à l'échelle d'un test d'intrusion spécifique

Audience :

- Professionnels informatiques souhaitant améliorer leurs connaissances et leurs compétences techniques
- Auditeurs souhaitant comprendre les processus du test d'intrusion
- Responsables des technologies de l'information et de gestion de risques souhaitant acquérir une compréhension plus détaillée de l'utilisation appropriée et bénéfique des tests d'intrusion
- Consultant Pen Testeurs
- Professionnels de la cybersécurité

Prérequis : Des connaissances de bases sur la sécurité de l'information.

Contenu de la formation :

1- Introduction aux tests d'intrusions, à l'éthique, à la planification et au domaine d'application

- Principes relatifs au test d'intrusion
- Questions légales et éthiques
- Principes fondamentaux de la sécurité de l'information et de la gestion des risques
- Approches de test d'intrusion
- Phases de test d'intrusion
- Gestion d'un test d'intrusion

2- Connaissances techniques fondamentales et techniques (avec des exercices pratiques dans tous les domaines)

- Connaissances techniques de base

3- Réalisation d'un test d'intrusion (à l'aide d'outils et de techniques) et revue du domaine du test

- Réalisation d'un test d'intrusion - Tester l'infrastructure
- Réalisation d'un test d'intrusion - Tests d'intrusion sur les applications Web
- Réalisation d'un test d'intrusion - Test mobile
- Réalisation d'un test d'intrusion - Tests d'ingénierie sociale

- Réalisation d'un test d’intrusion - Tests de sécurité physique

4- Analyse des résultats des tests, rapports et suivi
- Documentation de la revue de la qualité du test et du rapport
- Plans d'action et suivi
- Gestion d'un programme de test
- Compétence et évaluation des testeurs d’intrusion
- Exercices Capture the Flag CTF
- Clôture de la formation

5- Examen

ISO 22301 Foundation

Durée : 2 jours

Objectifs :
- Reconnaître la corrélation entre ISO 22301 et les autres normes et cadres réglementaires
- Comprendre les composantes et le fonctionnement d'un SMCA basé sur ISO 22301 et ses principaux processus
- Comprendre les concepts, les approches, les méthodes et les techniques utilisés pour la mise en œuvre et la gestion d'un SMCA

Audience :
- Les personnes impliquées dans la continuité d'activité
- Les personnes souhaitant acquérir des connaissances sur les principaux processus des systèmes de management de la continuité d'activité (SMCA)
- Les personnes souhaitant poursuivre une carrière dans la continuité d'activité

Prérequis : Aucun

Contenu de la formation :

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

- Introduction à la famille des normes ISO 22301.
- Principes fondamentaux en continuité d’activités
- Exigences générales : présentation des clauses 4 à 10 de la norme ISO 22301
- Phases de mise en œuvre du cadre ISO 22301.
- Amélioration continue de la Continuité d’activité.
- Conduire un audit de certification ISO 22301

2- Système de management de la continuité d'activité et examen de certification

ISO 22301 Lead Auditor

Durée : 5 jours

Objectifs :
- Comprendre la relation entre le système de management de la continuité d’activité, le management des risques et les mesures.

- Comprendre les principes, procédures et techniques d'audit de la norme ISO 19011 :2018, et comment les appliquer dans le cadre d'un audit selon la norme ISO 22301.
- Acquérir les compétences nécessaires pour auditer un SMCA conformément aux exigences de la norme ISO 22301, et les techniques de gestion d'une équipe d'audit.
- Préparer et compléter un rapport d'audit ISO 22301

Audience :

- Auditeur interne
- Equipe de contrôle interne
- Personne désirant diriger des audits de certification ISO 22301 en tant que responsable d'une équipe d'audit
- Consultant désirant préparer et accompagner une organisation lors d'un audit de certification ISO 22301

Prérequis : Une connaissance préalable de la norme ISO 22301 est recommandée

Contenu de la formation :

1- Introduction à la gestion d'un système de management de la sécurité de l'information selon ISO 22301

- Cadre normatif et réglementaire
- Processus de certification ISO 22301
- Principes fondamentaux de la continuité d'activités et de la gestion des risques
- Système de management de la continuité d'activités (SMCA).
- Présentation des clauses 4 à 10 de la norme ISO 22301

2- Démarrer un audit ISO 22301

- Concepts et principes fondamentaux d'audit
- Éthique et déontologie d'audit
- L'approche d'audit fondée sur la preuve et sur le risque
- Préparation d'un audit de certification ISO 22301
- L'audit documentaire
- Préparation du plan d'audit.
- Conduite d'une réunion d'ouverture.

3- Conduire un audit ISO 22301

- Communication durant l'audit
- Les procédures d'audit (observation, entrevue, techniques d'échantillonnage).
- Rédaction des conclusions d'audit et des rapports de non-conformité

4- Conclure un audit ISO 22301

- Documentation d'audit
- Revue des notes d'audit
- Conclusion d'un audit ISO 22301
- Gestion d'un programme d'audit
- La compétence et l'évaluation des auditeurs.
- Clôture de l'audit.

5- Examen

ISO 22301 Lead Implementer

Durée : 5 jours

Objectifs :

- Acquérir une compréhension globale des concepts, approches, méthodes et techniques utilisés pour la mise en œuvre et la gestion efficace d'un SMCA
- Apprendre à interpréter et à mettre en œuvre les exigences d'ISO 22301 dans le contexte spécifique d'un organisme
- Comprendre le fonctionnement du système de management de la continuité d'activité et ses processus basés sur ISO 22301
- Acquérir les connaissances nécessaires pour aider une entreprise à planifier, mettre en œuvre, gérer, contrôler et améliorer en permanence un SMCA

Audience :

- Les responsables de projets et les consultants impliqués dans la continuité d'activité
- Les conseillers experts cherchant à maîtriser la mise en œuvre du système de management de la continuité d'activité
- Les personnes chargées de maintenir la conformité aux exigences du SMCA au sein d'un organisme
- Les membres de l'équipe du SMCA

Prérequis : Une connaissance préalable des normes ISO 27001 et ISO 27002 est recommandée

Contenu de la formation :

1- Introduction à l'ISO 22301 et déclanchement d'un SMCA

- Objectifs et structure de la formation
- Normes des systèmes de management
- Principes et concepts fondamentaux de la continuité d'activité
- Système de management de la continuité d'activité
- Déclenchement de la mise en œuvre du SMCA
- Compréhension de l'organisme et de son contexte
- Analyse du système existant
- Périmètre du SMCA

2- Plan de mise en œuvre d'un SMCA

- Concepts et principes fondamentaux d'audit
- Leadership et engagement
- Objectifs de continuité d'activité et planification des changements
- Politique de continuité d'activité
- Structure organisationnelle
- Gestion de l'information documentée
- Compétence et sensibilisation
- Analyse d'impact sur les activités

3- Mise en œuvre d'un SMCA

- Évaluation des risques
- Stratégies et solutions de continuité d'activité
- Plans et procédures de continuité d'activité
- Plan d'intervention en cas d'incident
- Plan d'intervention d'urgence
- Plan de gestion de crise
- Communication

4- Suivi du SMCA, amélioration continue et préparation à l'audit de certification

- Programmes d'exercices
- Surveillance, mesure, analyse et évaluation

- Audit interne
- Revue de direction
- Traitement des non-conformités
- Amélioration continue
- Préparation à l'audit de certification
- Processus de certification et clôture de la formation

5- Examen

RGPD Foundation

Durée : 2 jours

Objectifs :

- Comprendre les exigences du règlement général sur la protection des données et les concepts fondamentaux de protection de la vie privée h Comprendre les obligations, les rôles et les responsabilités du délégué à la protection des données DPO
- Comprendre les concepts, les approches, les méthodes et les techniques pour aligner efficacement un cadre de conformité en ce qui concerne la protection des données personnelles.

Audience :

- Personnes impliquées dans la protection des données personnelles et la sécurité de l'information
- Personnes cherchant à acquérir des connaissances sur les principes essentiels de protection de la vie privée
- personnes intéressées à poursuivre une carrière dans le domaine de la protection des données

Prérequis : Aucun

Contenu de la formation :

1 - : Introduction aux principes de protection des données et du RGPD

2- Les exigences du règlement général sur la protection des données et l'examen de certification

Data Protection Officer

Durée : 5 jours

Objectifs :

- Acquérir une compréhension approfondie des concepts fondamentaux et des éléments du Règlement sur la protection des données
- Comprendre l'objectif, le contenu et la corrélation entre le Règlement général sur la protection des données et les autres cadres réglementaires
- Acquérir une compréhension approfondie des concepts, des approches, des méthodes et des techniques permettant une protection efficace des données à caractère personnel
- Savoir interpréter les exigences relatives à la protection des données dans le contexte particulier d'un organisme
- Acquérir l'expertise nécessaire pour aider un organisme à planifier, mettre en œuvre, gérer, surveiller et maintenir un cadre de conformité en ce qui concerne le RGPD

Audience :

- Responsables de projets et consultants qui désirent préparer et aider un organisme à mettre en œuvre les nouvelles procédures et à adopter les nouvelles exigences présentées dans le RGPD
- Délégués à la protection des données et membres de la direction générale responsables de la protection des données à caractère personnel d'une entreprise et de la gestion de ses risques
- Membres d'équipes de sécurité de l'information, de gestion des incidents et de continuité des activités
- Conseillers spécialisés en sécurité des données à caractère personnel
- Spécialistes des questions techniques et de conformité qui désirent se préparer à occuper un poste de délégué à la protection des données

Prérequis : Une connaissance préalable des normes ISO 27001 et ISO 27002 est recommandée

Contenu de la formation :

1- Introduction au RGPD et mise en œuvre de la conformité au RGPD

- Règlement général sur la protection des données
- Principes fondamentaux du RGPD
- Débuter la mise en place du RGPD
- Comprendre l'organisme et clarifier les objectifs de la protection des données
- Analyse du système actuel

2- Planification de la mise œuvre du RGPD

- Direction et approbation du projet de conformité du RGPD
- Politique de protection des données
- Définition de la structure organisationnelle de la protection des données
- Classification des données
- Évaluation des risques en vertu du RGPD

3- Déploiement des exigences du RGPD

- Analyse d'impact sur la protection des données
- Conception des mesures de sécurité et rédaction de politiques et de procédures spécifiques
- Mise en œuvre des mesures de sécurité
- Définition du processus de gestion des documents
- Plan de communication

4- Surveillance et amélioration continue de la conformité au RGPD

- Plan de formation et de sensibilisation
- Gestion des opérations
- Gestion des incidents
- Surveillance, mesure, analyse et évaluation
- Audit interne
- Violation des données et actions correctives
- Amélioration continue

5- Examen

Etat de l'art de la sécurité informatique

Durée : 3 jours

Objectifs :

- Reconnaître les divers domaines de la sécurité et de la gestion des risques liés aux informations
- Intégrer les normes et les principes de chaque domaine de la sécurité des systèmes d'informations
- Avoir en sa possession des données actualisées sur les tendances de menaces ou de solutions en matière de SSI
- Optimiser les échanges d'informations entre la maîtrise d'ouvrage, la maîtrise d'œuvre et la SSI
- Rendre les choix techniques moins problématiques et plus faciles au sein de son organisation

Audience :

- Directeurs des SI
- Responsables informatiques
- RSSI
- Chefs de projet sécurité
- Architectes informatiques

Prérequis :

- Aucun

Contenu de la formation :

Aperçu des menaces et des risques auxquels sont les SSI

- Statistiques et dégagement de tendances dans l'évolution des menaces de sécurité sur les SI
    - Traitement du risque
    - Validation des risques résiduels

Sécurité Windows

Durée : 3 jours

Objectifs :

- Savoir durcir et exploiter le démarrage d'un système
- Savoir durcir et exploiter un environnement Windows
- Connaître les méthodes d'attaques d'un Active Directory et comment s'en protéger
- Savoir durcir et exploiter les services Windows

Audience :

- Auditeurs techniques
- Administrateurs système

Prérequis :

- Notions de sécurité informatique
- Connaissance des protocoles réseaux TCP/IP
- Maîtrise des systèmes Windows (client et serveur) et Active Directory
- Savoir développer des scripts.

Contenu de la formation :

Domaine 1 – Menaces sur les systèmes d'exploitation Windows

- Chronologie et évolutions majeures des systèmes d'exploitation Windows
- Les attaques courantes dans un domaine Windows
- Segmentation des phases d'un attaquant

Domaine 2 - Durcissement des domaines Windows

- Stratégies de contrôle d'applications (AppLocker)
- Cohérence et défauts de conception de la structure Active Directory (ACL)
- Recommandations de sécurité pour Active Directory (bonnes pratiques)

Domaine 3 – Sécurité des services Windows

- Utilisation d'une infrastructure de clés publiques (PKI) pour la création de stratégies de sécurité réseau (Network Policy Server et Radius)
- Sécurisation de l'administration du domaine
    - WinRM (Windows Remote Management)
    - RPC (Remote Desktop Services)
    - WMI (Windows Management Instrumentation)
    - RDP (Remote Desktop Protocol)
- Sécurité des services et comptes de services managés
- Audit et centralisation des journaux d'évènements Windows

Domaine 4 – Durcissement des serveurs et postes clients

- Sécurisation du démarrage (Secure Boot - UEFI : Unified Extensible Firmware Interface)
    - Chiffrement des disques durs
    - Bitlocker
    - TPM (Trusted Platform Module)
    - Agent de récupération
- Pare-feu Windows (configuration et règles)
- Contrôler l'élévation de privilèges (UAC : User Account Control)
- Sécurisation des contenus Web (Smartscreen)
- Windows Defender
- Fonctionnalités antivirales
- Augmentation de la maîtrise de PowerShell

NOS CURSUS

Métier RSSI
Durée : 13 jours
Objectifs : • Acquérir les compétences nécessaires à la prise de fonction du rôle de RSSI d'une organisation
Audience : • RSSI nouvellement nommés • Aspirants au métier RSSI
Prérequis : • Notions de sécurité informatique
Contenu de la formation : **Domaine 1 – Etat de l'art de la sécurité** **Domaine 2 – ISO 27001 Lead Implementer** **Domaine 3 – Lead Pen Test Professionnel**

Métier Auditeur sécurité des SI
Durée : 13 jours
Objectifs : • Acquérir les compétences nécessaires à la prise de fonction du rôle d'Auditeur sécurité SI d'une organisation
Audience : • Auditeurs SI désirant renforcer ses capacités d'audit sécurité • Aspirants au métier d'auditeurs
Prérequis : • Notions de sécurité informatique • Notions en audit
Contenu de la formation : **Domaine 1 – Etat de l'art de la sécurité** **Domaine 2 – ISO 27001 Lead Auditor** **Domaine 3 – Lead Pen Test Professionnel**

Métier Consultant sécurité des SI
Durée : 13 jours
Objectifs : • Acquérir les compétences nécessaires pour exercer le métier de consultant en cybersécurité
Audience : • Profils désirant se reconvertir • Consultants désirant renforcer leurs compétences en termes de consulting en cybersécurité
Prérequis : • Notions de sécurité informatique

Contenu de la formation :
Domaine 1 – Métier du consultant

Domaine 2 – ISO 27001 Lead Implementer

Domaine 3 – ISO 27001 Lead Auditor