COETRIC

Centre de Formation professionnelle

Infoline : **+225 05 01 20 18 14**
Email: **formations@coetric.com**

COETRIC

À propos de nous

COETRIC est une société mise en place par des professionnels ayant de nombreuses expériences dans le domaine de la cybersécurité et la gouvernance IT. Notre fierté se trouve dans la qualité et l'expertise de notre ressource humaine de classe mondiale.
COETRIC ambitionne de devenir un centre d'excellence pour la formation professionnelle en Afrique de l'Ouest.

Nos services

COETRIC met à votre disposition les services ci-dessous :

Formations en cybersécurité et Gouvernance de la sécurité.
Sensibilisation du personnelle sur la sécurité.
Service d'audit informatique et Sécurité.
Mise en place de système de management de la sécurité de l'information SMSI (ISO 27001).
Mise en place de système de management de continuité d'activité SMCA (ISO 22301).

Nos Programmes de formation

01. CISA - Certified Information Systems Auditor
02. CISM - Certified Information Security Manager
03. CRISC - Certified in Risk and Information Systems Control
04. CISSP - Certified Information Systems Security Professional
05. CCSP – Certified Cloud Security Professional
06. ISO 27001 Lead Implementer
07. ISO 27001 Lead Auditor
08. ISO 27001 Transition
09. ISO 27005 Lead Risk Manager
10. ISO 22301 Lead Implementer
11. ISO 22301 Lead Auditor
12. ISO 27032 Lead Cybersecurity Manager
13. ITIL 4 Foundation
14. COBIT 2019 Foundation

CISA Certified Information Systems Auditor

Validez votre expertise et obtenez l'effet de levier dont vous avez besoin pour progresser dans votre carrière. Avec la certification Certified Information Systems Auditor (CISA) de l'ISACA, vous pouvez faire exactement cela. CISA est reconnu mondialement comme la norme de réalisation pour ceux qui auditent, contrôlent, surveillent et évaluent les technologies de l'information et les systèmes d'affaires d'une organisation.

CISA mets en valeur votre expertise et affirme votre capacité à appliquer une approche fondée sur les risques à la planification, à l'exécution et à la production de rapports sur les missions d'audit.

Objectifs de la formation

Que vous soyez à la recherche d'une nouvelle opportunité de carrière ou que vous vous efforciez de grandir au sein de votre organisation actuelle, cette formation prouve votre expertise dans ces domaines liés au travail :

- **Domaine 1:** Processus d'audit des systèmes d'information
- **Domaine 2:** Gouvernance et gestion de l'informatique
- **Domaine 3:** Acquisition, développement et mise en oeuvre de systèmes d'information
- **Domaine 4:** Exploitation des systèmes d'information et résilience des activités
- **Domaine 5:** Protection des actifs informationnels

Nombre de jours : 5 jours

Public

- Auditeurs
- Informaticiens ou personnes intervenants en audit des systèmes d'information

CISM Certified Information Security Manager

L'exfiltration de données, les attaques de rançongiciels et d'autres menaces de sécurité en constante évolution sont au cœur des préoccupations des professionnels de l'informatique d'aujourd'hui. Avec une certification Certified Information Security Manager® (CISM®), vous apprendrez à évaluer les risques, à mettre en œuvre une gouvernance efficace et à réagir de manière proactive aux incidents.

Objectifs de la formation

Cette formation CISM vous fournit une expertise dans la gouvernance de la sécurité de l'information, le développement et la gestion de programmes, la gestion des incidents et la gestion des risques. La formation CISM prouve votre expertise dans ces domaines liés au travail.

- **Domaine 1:** Gouvernance de la sécurité de l'information.
- **Domaine 2:** Gestion des risques liés à la sécurité de l'information.
- **Domaine 3:** Programme de sécurité de l'information.
- **Domaine 4:** Gestion des incidents.

Nombre de jours : 5 jours

Public

La certification Certified Information Security Manager (CISM) de l'ISACA est destinée à ceux qui ont une expertise technique et une expérience en sécurité et contrôle IS/IT et qui souhaitent devenir manager de la sécurité de l'information.

CRISC
Certified in Risk and Information Systems Control

Certified in Risk and Information Systems Control (CRISC) reflète les dernières pratiques de travail et connaissances utilisées par les praticiens CRISC, les changements dans le paysage commercial et l'accent accru mis sur la gouvernance d'entreprise et l'amélioration de la résilience des entreprises. Les employeurs peuvent être assurés qu'armés de CRISC, leur équipe informatique suit les meilleures pratiques de gouvernance et adopte une approche proactive et agile de la GITI qui atténue les risques et les menaces et optimise les ressources et le retour sur investissement.

Objectifs de la formation

Cette formation développe vos compétences en :

- **Domaine 1:** Gouvernance
- **Domaine 2:** Évaluation des risques informatiques
- **Domaine 3:** Réponse aux risques et rapports
- **Domaine 4:** Technologie de l'information et sécurité

Nombre de jours : 5 jours

Public

- Professionnels de l'audit IT/IS
- Professionnels du risque
- Professionnels du contrôle
- Les analystes
- et chefs de projet

CISSP
Certified Information Systems Security Professional

Le CISSP est l'une des certifications professionnelles les plus recherchées disponibles dans l'industrie de la sécurité. L'acronyme CISSP signifie Certified Information Systems Security Professional et a été créé pour démontrer qu'un professionnel de la sécurité est capable de concevoir, de mettre en œuvre et d'exécuter un programme de sécurité de l'information.

Objectifs de la formation

A l'issue de cette formation dispensée par un formateur agréé (ISC)², vous devrez être capable de valider les objectifs de compétences suivants :

- Connaître les différents domaines du CBK (Common Body of Knowledge)
- défini par l'(ISC)².
- Obtenir les connaissances fondamentales concernant la sécurité et gestion des
- risques, sécurité des actifs, architecture et ingénierie de la sécurité,
- communication et sécurité des réseaux, gestion des identités et des accès (IAM),
- évaluation et test de la sécurité, opérations de sécurité, sécurité du
- développement logiciel.

Nombre de jours : 5 jours

Public

- Responsable de la Sécurité des Systèmes de l'Information (RSSI)
- Directeur de la sécurité
- Directeur/Responsable IT
- Ingénieur Systèmes de Sécurité
- Analyste de sécurité
- Responsable de la sécurité
- Auditeur de sécurité
- Architecte de sécurité
- Consultant en sécurité
- Architecte réseau

CCSP Certified Cloud Security Professional

Le CCSP montre que vous possédez les compétences et les connaissances techniques avancées nécessaires pour concevoir, gérer et sécuriser les données, les applications et l'infrastructure dans le cloud en utilisant les meilleures pratiques, politiques et procédures établies par les experts en cybersécurité de (ISC)².

Objectifs de la formation

Cette formation vous fournit une expertise dans les domaines ci-dessous :

- Sécurité des applications cloud
- Concept d'architecture cloud
- Exigences de conformité cloud
- Sécurité des données dans le cloud
- Exigences de conception du cloud
- Sécurité de l'infrastructure du cloud
- Exigences légales en matière de cloud
- Operations cloud
- Sécurité de la plateforme cloud

Nombre de jours : 5 jours

Public

- Responsable de la Sécurité des Systèmes de l'Information (RSSI)
- Directeur de la sécurité
- Architecte Cloud
- Ingénieur Cloud
- Cloud Consultant
- Administrateur Cloud
- Analyste de la sécurité du cloud
- Spécialiste Cloud
- Auditeur des services de cloud computing
- Développeur Cloud professionnel

ISO 27001 Lead Implementer

Cette formation est conçue pour vous préparer à la mise en œuvre Système de Management de la Sécurité de l'Information (SMSI) conformément aux exigences de la norme ISO/IEC 27001. Elle vise à donner une compréhension complète des bonnes pratiquesd'un SMSI et un cadre pour sa gestion et son amélioration continue.
La formation comprend de nombreux exercices pratiques et études de cas qui vous permettront d'acquérir une expertise concrète que vous pourrez appliquer à vos opérations et activités quotidiennes.

Objectifs de la formation

Cette formation vous permet :

- D'acquérir une compréhension complète des concepts, approches, méthodes et techniques utilisés pour la mise en oeuvre et le management efficace d'un SMSI.
- De comprendre la corrélation entre les normes ISO/IEC 27001, ISO/IEC 27002 et d'autres normes et cadres réglementaires.
- De comprendre le fonctionnement d'un système de management de la sécurité de l'information et ses processus conformément à la norme ISO/IEC 2700.
- D'apprendre à interpréter et à mettre en oeuvre les exigences d'ISO/IEC 27001 dans le contexte spécifique d'un organisme.
- De développer les connaissances et les compétences nécessaires pour aider un organisme à planifier, mettre en oeuvre, gérer, surveiller et maintenir efficacement un SMSI.

Nombre de jours : 5 jours

Public

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

ISO 27001 Lead Auditor

La formation ISO/IEC 27001 Lead Auditor vous permet de développer l'expertise nécessaire à la réalisation d'un audit de Système de Management de la Sécurité de l'Information (SMSI) en appliquant des principes, procédures et techniques largement reconnus en audit. Au cours de cette formation, vous acquerrez les connaissances et les compétences nécessaires pour planifier et réaliser des audits internes et externes conformément aux processus de certification ISO 19011 et ISO/IEC 17021-1. Sur la base d'exercices pratiques, vous maîtriserez les techniques d'audit et la gestion d'un programme d'audit, d'une équipe d'audit, la communication avec les clients et la résolution de conflits.

Objectifs de la formation

À l'issue de cette formation, les participants seront capables :

- D'expliquer les concepts et les principes fondamentaux d'un système de management de la sécurité de l'information (SMSI) basé sur ISO 27001.
- D'interpréter les exigences d'ISO 27001 pour un SMSI du point de vue d'un auditeur.
- D'évaluer la conformité du SMSI aux exigences d'ISO 27001, en accord avec les concepts et les principes fondamentaux d'audit.
- De planifier, réaliser et clôturer un audit de conformité à ISO 27001, conformément aux exigences d'ISO/IEC 17021-1, aux lignes directrices d'ISO 19011 et aux autres bonnes pratiques d'audit.
- De gérer un programme d'audit ISO/IEC 27001.

Nombre de jours : 5 jours

Public

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

ISO 27001 Transition

La formation ISO/IEC 27001 Transition permet aux participants de bien comprendre les différences entre ISO/IEC 27001:2013 et ISO/IEC 27001:2022. En outre, les participants acquerront des connaissances sur les nouveaux concepts présentés par ISO/IEC 27001:2022.
Le cours de formation « PECB ISO/IEC 27001 Transition » fournit des informations détaillées sur les clauses révisées, la nouvelle terminologie et les différences dans les contrôles de l'Annexe A. En outre, ce cours de formation fournit aux participants les connaissances nécessaires pour aider les organisations à planifier et à mettre en œuvre les changements dans leur SMSI afin d'assurer la conformité à la norme ISO/IEC 27001:2022.

Objectifs de la formation

Après avoir terminé avec succès le cours de formation, les participants seront en mesure :

- D'expliquer les différences entre ISO/IEC 27001:2013 et ISO/IEC 27001:2022
- D'interpréter les nouveaux concepts et exigences de l'ISO/IEC 27001:2022
- De planifier et mettre en œuvre les modifications nécessaires à un SMSI existant
- conformément à la norme ISO/IEC 27001:2022.

Nombre de jours : 2 jours

Public

- Personnes souhaitant rester à jour avec les exigences ISO/IEC 27001 pour un SMSI.
- Personnes cherchant à comprendre les différences entre les exigences ISO/IEC 27001:2013 et ISO/IEC 27001:2022.
- Personnes responsables de la transition d'un SMSI de l'ISO/IEC 27001:2013 à l'ISO/IEC 27001:2022.
- Gestionnaires, formateurs et consultants impliqués dans la maintenance d'un SMSI.
- Professionnels souhaitant mettre à jour leurs certificats ISO/IEC 27001.

ISO 27005
Lead Risk Manager

L'ISO / IEC 27005 fournit les lignes directrices pour l'établissement d'une approche systématique de la gestion des risques liés à la sécurité de l'information laquelle est nécessaire pour identifier les besoins organisationnels en matière de sécurité de l'information et pour créer un système efficace de management de la sécurité de l'information.
Elle prouve que vous êtes en mesure d'identifier, d'apprécier, d'analyser, d'évaluer et de traiter les divers risques de sécurité de l'information auxquels font face les organisations.En outre, elle vous donne l'expertise nécessaire pour accompagner les organisations à hiérarchiser leurs risques et d'entreprendre des actions appropriées pour les réduire et les atténuer.

Objectifs de la formation

La certification PECB ISO/IEC 27005 de 4 jours démontre que vous avez :

- Obtenu 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.
- Acquis l'expertise nécessaire pour gérer de façon responsable un processus de gestion des risques liés à la sécurité de l'information et assurer la conformité aux exigences légales et réglementaires.
- La capacité à gérer une équipe de sécurité de l'information et de management du risque.
- L'aptitude à aider une organisation à aligner ses objectifs du SMSI sur les objectifs du processus de Gestion des risques liés à la sécurité de l'information (GRSI).

Nombre de jours : 4 jours

Public

- 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 un organisme
- Tout individu mettant en œuvre ISO/IEC 27001, désirant se conformer à la norme ISO/IEC 27001 ou impliqué dans un programme de management du risque
- Consultants et professionnel IT
- Responsables de la protection de la vie privée

ISO 22301 Lead Implementer

La formation ISO 22301 Lead Implementer vous permettra d'acquérir l'expertise nécessaire pour accompagner une organisation lors de l'établissement, la mise en œuvre, la gestion et la tenue à jour d'un Système de Management de la Continuité d'Activité (SMCA) conforme à la norme ISO 22301. Cette formation est conçue de manière à vous doter d'une maîtrise des meilleures pratiques en matière de Systèmes de management de la continuité d'activité et à développer vos aptitudes à fournir un cadre qui permet à l'organisation de continuer ses activités durant les crises.

Objectifs de la formation

À la fin de cette formation de 5 jours, les participants seront en mesure :

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

Nombre de jours : 5 jours

Public

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

ISO 22301 Lead Auditor

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

Objectifs de la formation

À la fin de cette formation, les participants seront en mesure :

- D'expliquer les concepts et principes fondamentaux d'un système de management de la continuité d'activité (SMCA) basé sur ISO 22301.
- D'interpréter les exigences d'ISO 22301 pour un SMCA du point de vue d'un auditeur.
- D'évaluer la conformité du SMCA aux exigences d'ISO 22301, en accord avec les concepts et principes fondamentaux d'audit.
- De planifier, conduire et clore un audit de conformité à ISO 22301, conformément aux exigences d'ISO/IEC 17021-1, aux lignes directrices d'ISO 19011 et aux autres bonnes pratiques d'audit.
- De gérer un programme d'audit ISO 22301.

Nombre de jours : 5 jours

Public

- Auditeurs souhaitant réaliser et diriger des audits de certification du Système de management de la continuité d'activité.
- Responsables ou consultants désirant maîtriser le processus d'audit du Système de Management de la Continuité d'Activité.
- Toute personne responsable du maintien de la conformité aux exigences du SMCA.
- Experts techniques désirant préparer un audit du Système de Management de la Continuité d'Activité.

ISO 27032 Lead Cybersecurity Manager

La norme ISO/IEC 27032 fait référence à la «cybersécurité» ou à la «sécurité du cyberespace», qui est définie comme la protection de la vie privée, de l'intégrité et de l'accessibilité des données dans le cyberespace. Par conséquent, le cyberespace est reconnu comme une interaction de personnes, de logiciels et de services technologiques mondiaux.
La formation ISO / IEC 27032 Lead Cybersecurity fournit une solution réaliste aux individus dans la protection de leurs données privées et pour la protection des données des organisations contre les escroqueries de phishing, les cyberattaques, le piratage informatique, les violations de données, les logiciels espions, l'espionnage, le sabotage et autres menaces cybernétiques. Être certifié ISO / IEC 27032 démontrera à vos clients et parties prenantes que vous pouvez gérer et fournir des solutions à leurs problèmes de cybersécurité.

Objectifs de la formation

Devenir un professionnel certifié ISO/IEC 27032 Lead Cybersecurity Manager vous permet :

- De protéger les données et la confidentialité d'une organisation contre les menaces cybernétiques.
- De renforcer vos compétences dans la mise en place et la maintenance d'un programme de cybersécurité.
- De développer les bonnes pratiques pour gérer les politiques de cybersécurité
- D'améliorer le système de sécurité de l'organisation et assurer sa continuité d'activité.
- D'assurer la confiance des parties prenantes en vos mesures de sécurité.
- De réagir et récupérer plus rapidement en cas d'incident.

Nombre de jours : 5 jours

Public

- Toute personne impliquée dans un programme de cybersécurité.
- Tout professionnel souhaitant enrichir ses compétences et techniques en cybersécurité.
- Tout professionnel de la sécurité et des technologies de l'information.
- Les consultants en sécurité et technologies de l'information.

ITIL 4 Foundation

ITIL 4 Foundation c'est un référentiel de bonne pratique qui introduit un modèle d'exploitation de bout en bout pour la création, la livraison et l'amélioration continue de produits et services technologiques.
ITIL 4 Foundation s'adresse à tous ceux qui ont besoin de comprendre les concepts clés de la prestation de services informatiques et numériques, et qui souhaitent aider leur organisation à adopter la nouvelle culture de gestion des services.

Objectifs de la formation

Devenir un professionnel certifié ISO/IEC 27032 Lead Cybersecurity Manager vous permet de :

- Comprendre les concepts clés de la gestion des services.
- Comprendre comment les principes directeurs d'ITIL peuvent aider une organisation à adopter et à adapter la gestion des services.
- Comprendre les quatre dimensions de la gestion des services.
- Comprendre le but et les composants du système de valeur des services ITIL.
- Comprendre les activités de la chaîne de valeur des services, et leurs interconnexions
- Connaître le but et les termes clés de 15 pratiques ITIL.
- Comprendre 7 pratiques ITIL.
- Se préparer et passer la certification ITIL 4 Foundation.

Nombre de jours : 3 jours

Public

- Directeur des Systèmes d'Information (DSI)
- Tous professionnels impliqués au sein d'un service informatique
- Toutes personnes interagissant avec des services informatiques
- Toutes personnes souhaitant connaître la gestion des services informatiques
- Chef de projet / Responsable de projet informatique

COBIT 2019 Foundation

Lorsqu'il s'agit de gérer des services et des équipes informatiques, les dirigeants doivent être prêts à s'adapter à tous les composants et considérations pertinents. L'adoption des outils, des pratiques et des structures appropriés pour favoriser l'optimisation nécessite une perspective globale et souvent de haut niveau. C'est là qu'intervient COBIT 2019.
COBIT est un référentiel de bonnes pratiques d'audit informatique et de gouvernance des systèmes d'information.

Objectifs de la formation

- Comprendre les enjeux de la gouvernance du Système d'Information.
- Connaître la structure du référentiel COBIT.
- Evaluer la capacité d'un processus avec le Process Assessment Model.
- Se préparer à l'examen de certification COBIT Foundation.

Nombre de jours : 3 jours

Public

- Responsables de la sécurité de l'information
- Membres de la DSI
- Directeurs des systèmes d'information
- Directeurs exécutifs
- Directeurs métiers
- Auditeurs IT/IS.
- Contrôleurs internes
- Consultants

Avez-vous des questions ?

NOUS CONTACTER

Angré 9eme Tranche, Cocody
04 BP 2257 Abidjan 04

Email: formations@coetric.com
Tel : +225 05 01 20 18 14
www.coetric.com