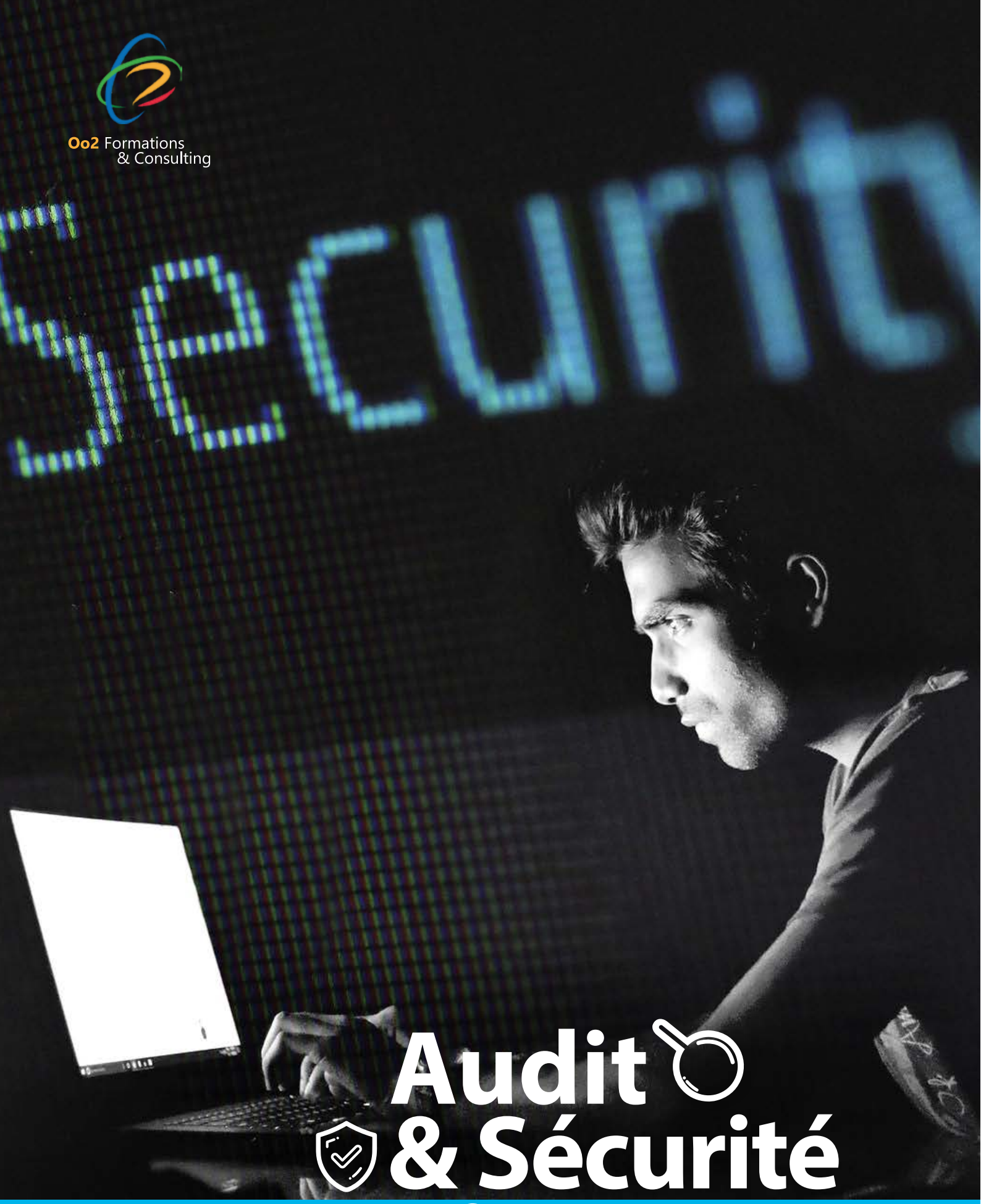
Oo2 Formations
& Consulting

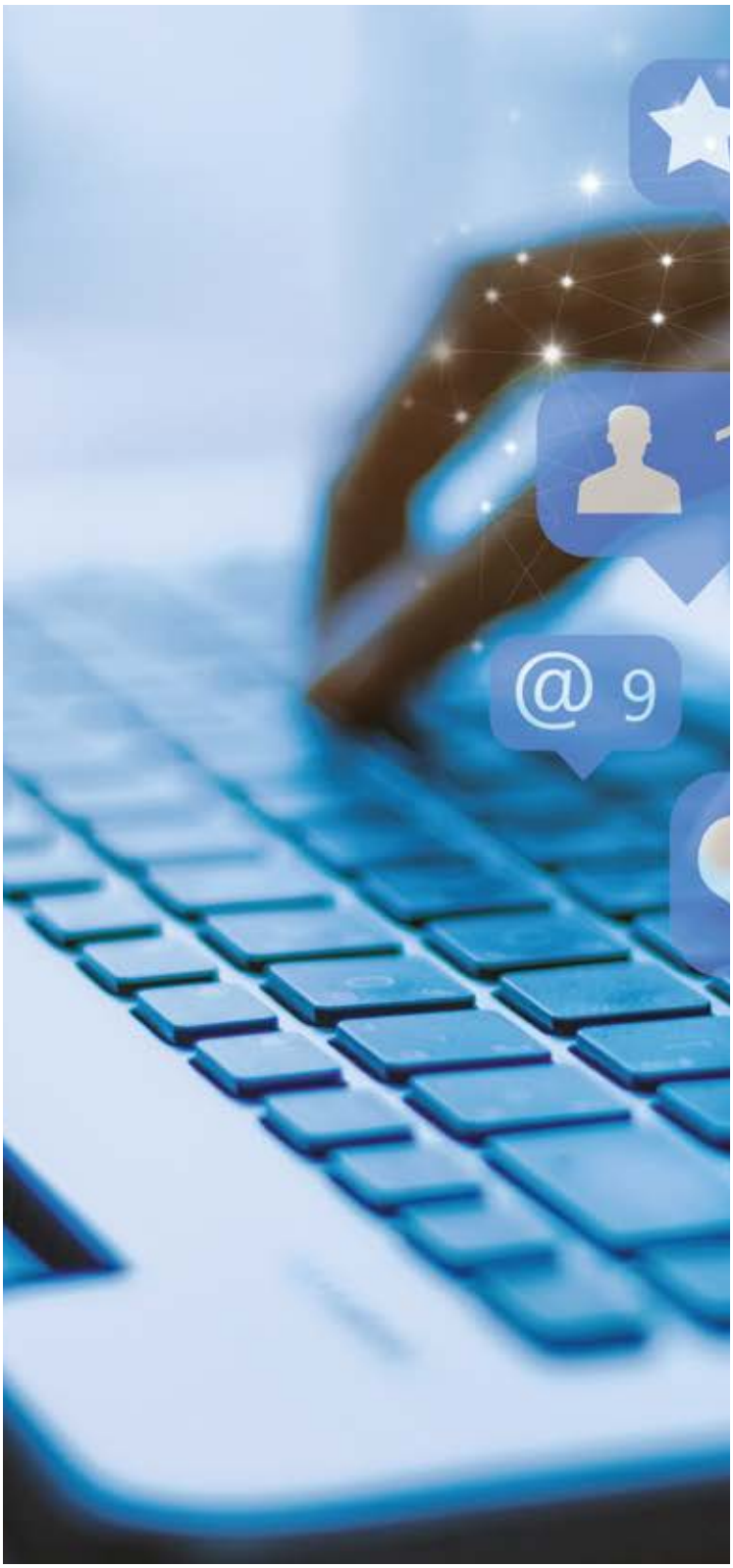


Audit & Sécurité Informatique

Formations et certifications internationales

Sommaire

Audit & sécurité informatique



L'avènement du numérique, le développement du web, le cloud computing et la connectivité des systèmes IT sont autant de facteurs qui peuvent conduire à un accroissement des risques pour les entreprises.

Qu'il s'agisse de menaces internes ou externes, veiller à la bonne sécurisation d'un système d'information est un élément majeur dans la bonne gouvernance d'une organisation.

En effet, un système d'information (SI) est l'ensemble des ressources qui interviennent dans la gestion de l'information. Par conséquent, il est important d'avoir une vue d'ensemble de la situation de ses ressources informatiques et de s'assurer que toutes soient sécurisées.

Dans cette brochure, vous trouverez un panorama de nos formations et certifications les plus pertinentes en matière de sécurité et d'audit informatiques. Chacune de ces formations vous permettra de trouver rapidement des solutions adaptées à votre structure pour identifier, traiter et finalement réduire votre exposition face aux risques informatiques actuels et futurs.

Audit de sécurité informatique :

Ce que vous devez savoir

L'audit de sécurité informatique, c'est quoi ?

L'audit de sécurité est un diagnostic permettant de révéler l'état de sécurité de votre système d'information. Il vise à mettre en évidence les éventuelles failles ou dysfonctionnements susceptibles de compromettre les activités de l'entreprise.

C'est également un processus qui vous permet d'évaluer le niveau de conformité par rapport à votre politique de sécurité et aux normes en matière de sécurité de l'information qui sont en vigueur.

L'audit de sécurité informatique garantit ainsi la disponibilité du système d'information, l'intégrité de vos données, la confidentialité des accès, et permet de déceler les vulnérabilités du SI afin d'en maitriser les risques.

L'audit de sécurité informatique, pour qui ?

A l'ère du digital, toutes les organisations disposent aujourd'hui d'un système d'information fortement dématérialisé. La sécurité informatique concerne donc toutes les organisations, les grandes comme les petites entreprises, les administrations et les associations.

Une faille ou une défaillance de la sécurité de votre SI peut mettre en risque la continuité de votre activité. Pour éviter de vous retrouver face à un verrouillage ou un vol de données, pensez à réaliser régulièrement des audits de sécurité informatique, car la prévention réduit fortement le risque. Qu'il s'agisse de gérer les risques internes (manque de sensibilisation des collaborateurs, erreurs, incidents, accès aux données critiques, malveillance, etc.) ou les risques externes (**virus, intrusions, phishing, espionnage**, etc.), la sécurité d'un **SI** est désormais un enjeu de taille dans la gouvernance de toute structure.

L'audit de sécurité informatique, pour faire quoi ?

Qu'il s'agisse d'un audit de sécurité organisationnel ou technique, l'audit de sécurité permet de mettre en évidence les faiblesses et les vulnérabilités du système d'information et de définir des axes d'amélioration pour en relever le niveau de sécurité.

En soi, un audit de sécurité informatique doit permettre d'atteindre les objectifs suivants :

- Évaluer le niveau de maturité du SI (analyse de l'architecture réseau, configuration, contrôle des accès, sécurité des ressources humaines et des communications, cryptographie…) ;
- Tester la résistance du SI face à une attaque ;
- Tester l'efficacité de la politique de sécurité du SI (PSSI) ;
- Vérifier la conformité du SI. Il pourra s'agir du respect des réglementations et obligations légales ainsi que de la conformité avec les référentiels en vigueur (ISO 27000, COBIT, ITIL, EBIOS, MEHARI, etc. et bien entendu les directives élaborées par l'agence nationale de sécurité de système d'information de votre pays, à défaut de l'ANSSI pour la France ;
- Tester l'intégration d'un nouvel équipement.

Afin de bénéficier d'une analyse exhaustive, Oo2 Consulting vous recommande de procéder à un audit complet : audit organisationnel et audit technique.

L'audit de sécurité informatique, comment ça se passe ?

Quel que soit l'audit de sécurité informatique que vous choisirez, le déroulement d'une mission d'audit s'organise plus ou moins selon le même enchainement de phases : la préparation de la mission d'audit, l'audit en lui-même et enfin les résultats de l'audit.

Les étapes d'un audit de sécurité informatique

Phase préparatoire : Organisation d'une réunion de cadrage entre Oo2, l'auditeur Oo2, l'organisme audité (vous) et éventuellement son commanditaire (s'il s'agit d'un audit externe). Cette rencontre doit permettre de définir les objectifs de l'audit, son périmètre, des critères d'audit, etc.

Phase d'exécution de l'audit : Réalisation des entretiens avec les personnes intéressées, analyse de l'architecture réseau, analyse des configurations, audit des vulnérabilités infrastructure et système, test éventuel d'intrusion. Analyse in fine des écarts entre les preuves fournies et les critères d'audit.

Phase de restitution : Oo2 vous transmet son rapport d'audit qui comprend des recommandations, présenté, au cours d'une réunion de clôture, à la Direction de votre entreprise ainsi qu'au DSI : il est important que les méthodes, constats et conclusions de l'audit soient bien compris par toutes les parties prenantes du projet.

L'audit de sécurité informatique, et après ?

Après l'audit de sécurité informatique, vient le temps des résultats restitués dans un rapport d'audit qui vous recommandera les optimisations prioritaires à faire pour assurer la sécurité de votre Système d'Information.

Ce document compile l'ensemble des failles de sécurité constatées et apporte les recommandations, classées par ordre de priorité. Dans ce contexte, Oo2 Consulting est en mesure de vous accompagner dans la mise en œuvre de ce plan d'action. Que ce soit en cas de manque de ressources internes ou dans le cas où ces recommandations impliquent un arrêt total ou partiel de vos services, il est nécessaire d'assurer la continuité de vos activités.

Attention, un audit de sécurité informatique donne une photographie à l'instant « T » du niveau d'efficacité global de la sécurité de votre SI. Le SI étant évolutif, il convient donc de réaliser (en interne, si les compétences le permettent) ou de faire réaliser (en externe par un prestataire tel que Oo2 Consulting) périodiquement un audit de sécurité.

Faire réaliser régulièrement des audits de sécurité informatique est la clé pour sécuriser les données de votre organisation.

...Quelques formations

en Audit de Sécurité Informatique

Fortinet NSE

FortiGate Network Security Professional

FORTINET

Attestez de vos compétences en sécurité et en architecture informatique avec la certification **Fortinet NSE**

La certification **Fortinet NSE** vous permet de :

- Neutraliser les menaces véhicules, les applications nocives et limiter les accès aux sites inappropriés
- Décrire les fonctionnalités des UTM du FortiGate et mettre en place différents VPN de type SSL ou IPSEC
- Définir des règles pour les firewalls, mettre en place des tunnels IPSEC
- Haute disponibilité : déployer un cluster, faire du load balancing et comprendre l'accélération matérielle
- Mettre en oeuvre les Virtual Domain, des politiques antiDoS, le FSS
- Maîtriser la mise en oeuvre de l'identification des utilisateurs ou l'authentification transparente dans les environnement Active Directory
- Diagnostiquer et résoudre des problématiques simples sur le FortiGate
- Mettre en place le routage avec le NAT/PAT

Avec des menaces informatiques de plus en plus sophistiquées et soutenues, les entreprises sont contraintes de s'équiper d'outils de sécurité complexes qu'il convient de déployer, d'administrer et de maintenir. Cette formation NSE découpée en deux parties FortiGate I & II vous permet de prendre en main les principales fonctions de l'UTM du FortiGate.

voir le programme >

CISSP®

Certified Information Systems Security Professional

Certified Information Systems Security Professional

Devenez expert de la sécurité informatique et réseaux grace à la certification **CISSP®**

Accompagnement à l'obtention de la **certification**

- Acquisition des connaissances nécessaires pour conseiller une organisation sur les meilleures pratiques en management de la sécurité de l'information
- Reconnaissance internationale des compétences en sécurité de l'information
- Maîtrise des connaissances en sécurité de l'information dans les dix domaines du CBK
- Compréhension des besoins en sécurité de l'information pour toute organisation
- Avoir les compétences et connaissances requises pour la réussite de l'examen et l'obtention de la certification
- Savoir dialoguer avec le management pour la mise en oeuvre des mesures de sécurité

Délivré par la fondation (ISC)2, le CISSP est l'une des certifications les plus reconnues et les plus prestigieuses dans le domaine de la sécurité des systèmes informatiques. Lancé en 1994, le premier titre de compétence offert par la fondation (ISC)2 est devenu incontournable et représente le titre de compétence par excellence de son éditeur et se positionne à la 4ème place des certifications les mieux rémunérées.

voir le programme >

Oo2 est accrédité **ATC** par

EC-Council

Oo2 est accrédité par EC-Council pour dispenser la formation CEH (Certified Ethical Hacker). Ce statut d'Oo2 garantit la prestation d'un formateur agrée, des supports de cours officiels et des examens de certification organisés immédiatement à la suite de la formation sur le lieu de formation ou en ligne

EC-Council est un organisme qui propose des certifications de haut niveau dans le domaine de l'informatique et de la cybersécurité. Le programme de certification EC-Council est accessible dans plus de 90 pays, et il est reconnu partout dans le monde.

Le réseau ATC de l'EC-Council est le canal le plus prometteur pour dispenser une formation de haute qualité en matière de sécurité de l'information destinée aux entreprises et professionnels du secteur.

Découvrez sur le site www.oo2.fr les dernieres certifications de l'EC-Council que vous pouvez préparer chez Oo2 Formations, un des rares organismes de formation professionnelle en Afrique à avoir obtenu cette prestigieuse accréditation.

scanner

CEH

Certified Hetical Haccker

Attestez de vos compétences en sécurité et en architecture informatique avec la certification **CEH**

La certification **CEH** vous permet de :

- Devélopper des compétences spécifiques en système et réseau informatique
- Connaitre et maîtriser les outils de hacking
- Maîtriser les méthodologies de piratage et d'intrusion éthique
- Comprendre les lois et l'éthique forte à respecter pour toute personne certifiée CEH
- Découvrir comment scanner, tester, hacker son propre système et détecter les intrusions et les faiblesses
- Comprendre comment fonctionne la défense périmétrique
- Acquérir les techniques et les outils nécessaires pour mettre en oeuvre un système de sécurité
- Connaitre et réaliser une démarche d'audit sécurité

C|EH Certified Ethical Hacker

Un Hacker Ethique Certifié est un professionnel qualifié qui comprend et sait comment rechercher les faiblesses et les vulnérabilités des systèmes d'information. Cette formation vous permet de développer vos compétences en informatique système et réseau, de connaitre les techniques de hacking et d'intrusion, d'identifier les faiblesses et vulnérabilités d'un système informatique et d'être sensibilisé sur les lois et éthique qui s'appliquent à tout CEH. Avec cette certification CEH, vous rejoindrez une communauté de professionnels internationaux rares et recherchés.

voir le programme >

CCISO

Chief Certified Information Security System de l'EC-Council

Avec la certification **CCISO**, certifiez vos connaissances et votre expertise en cybersecurity

La certification **CCISO** vous permet de :

- Mettre en place une structure de gestion de la sécurité de l'information, piloter les programmes de conformité et de gouvernance
- Comprendre l'architecture d'entreprise (EA) et la sécurité de la virtualisation
- Maîtriser les 5 grands domaines de compétences d'un Directeur des Systèmes d'Information (DSI) certifié
- Garantir la sécurité du réseau, les technologies de cryptage et la planification de la stratégie
- Contrôler la sécurité de l'information, gestion de l'audit et le contrôle d'accès
- Assurer la maintenance d'un programme de sécurité de l'information
- Maîtriser l'ensemble des enjeux exécutifs de la sécurité informatique : considérations politiques, gestion de projets, connaissance des lois et normes en vigueur
- Se préparer et réussir l'examen de certification CCISO

C|CISO
Certified | Chief Information Security Officer

La certification CCISO (Certified Chief Information Security Officer) de l'EC-Council, donne aux responsables de la sécurité de l'information (RSSI, DSI…) une reconnaissance internationale de leurs capacités et techniques à assurer au plus haut niveau la gestion de la sécurité de l'information au sein d'une organisation. Cette formation vous apportera toutes les connaissances nécessaires pour passer et réussir l'examen de certification CCISO.

voir le programme >

Les Quatre certifications

ISACA®

Les Quatre certifications d'ISACA

CISA Certified Information Systems Auditor® An ISACA® Certification

CISM Certified Information Security Manager® An ISACA® Certification

CGEIT Certified in the Governance of Enterprise IT® An ISACA® Certification

CRISC Certified in Risk and Information Systems Control™ An ISACA® Certification

ISACA® est une association internationale engagée dans le développement des pratiques de pointe en matière de systèmes d'information. Elle propose 4 certifications (CISA, CISM, CGEIT, CRISC) reconnues au niveau international dans les domaines de l'audit informatique, de la sécurité, de la gouvernance et des risques. Une certification ISACA confirme que vous possédez l'expérience et les connaissances nécessaires pour relever les défis de l'entreprise moderne et vous donne l'opportunité d'avancer dans votre carrière, d'augmenter votre potentiel de revenus et d'ajouter de la valeur à toute entreprise.

Validez vos connaissances et faites valoir vos compétences en audit informatique avec la CISA®

La CISA est une certification prestigieuse et reconnue mondialement par la communauté des experts de l'audit informatique. Proposée par l'ISACA, cette certification s'adresse aux professionnels des technologies occupant des fonctions liées à l'audit et à la gouvernance. La plupart des grandes entreprises (banques centrales, instituts financiers, etc.) travers le monde exigent cette certification pour la réalisation d'audits efficaces. La CISA atteste des connaissances et de la capacité du professionnel à évaluer, contrôler, auditer et effectuer une surveillance continue des systèmes informatiques de l'entreprise.

Préparation à la certification CISA®

Objectifs

- Être capable de mettre en oeuvre une politique et des mécanismes permettant de respecter les exigences en matière de gouvernance informatique en entreprise
- Maîtriser et savoir utiliser l'approche orientée risque de l'ISACA
- Connaître l'environnement réglementaire actuel de l'audit interne et externe
- Savoir mettre en oeuvre une architecture de sécurité (politiques, normes, procédures et contrôles)
- Garantir un plan de secours et de continuité d'activité en cas d'interruption pour permettre le rétablissement rapide des services informatiques
- Obtenir une reconnaissance internationale de vos connaissances et compétences en sécurité informatique

voir le programme >

Certifiez vos connaissances et votre expertise en management de la sécurité de l'information avec la CISM®

CISM (Certified Information Security Manager) est une certification qui s'adresse aux professionnels de la sécurité informatique. Délivrée par l'ISACA et détenue par 50000 professionnels à travers le monde dont plus de 7500 occupants des postes de CISO, RSSI, DSI. CISM fait partie des certifications les plus reconnues dans le domaine de la gouvernance des systèmes d'information.

Préparation à la certification CISM®

Objectifs

- Acquérir des compétences et connaissances techniques des technologies de l'information
- Maîtriser des concepts reliés à la gouvernance, au contrôle et à l'audit de sécurité des technologies de l'information
- Maîtriser des techniques informatiques de contrôle et de vérification dans un environnement informatique
- Assimiler de nouveaux outils d'analyse des risques reliés à l'utilisation des technologies de l'information
- Démontrer des compétences de base et des standards internationaux de performance attendus des responsables de la sécurité de l'information
- Avoir une bonne compréhension des différents domaines de progression sur lesquels porte l'examen

voir le programme >

Attestez vos aptitudes et connaissances en gouvernance des systèmes d'information avec la CGEIT®

La formation CGEIT vous apporte les compétences et les connaissances techniques pour manager la gouvernance des systèmes d'information en entreprise. Elle vous donne également les méthodes et pratiques de gouvernance IT, la gestion des risques, l'optimisation des ressources, etc. CGEIT est la certification la plus recherchée dans le domaine de la gouvernance des systèmes d'information et aussi la mieux rémunérée parmi toutes les autres certifications.

Préparation à la certification CGEIT®

Objectifs

- Assurer une gestion optimale des risques liés aux systèmes d'information
- Optimiser des ressources de l'entreprise tout en assurant la fiabilité et la sureté des systèmes d'information
- Soutenir et réaliser les objectifs de l'entreprise via l'appui des technologies informatiques
- Définir, établir et gérer le cadre de la gouvernance des systèmes d'information au sein d'une entreprise
- Appliquer les meilleures pratiques en gouvernance des SI dans une organisation et comprendre les outils et concepts de la gestion stratégique dans la gouvernance des SI
- Assurer une meilleure gestion de la stratégie de l'informatique et la concrétisation des bénéfices attendus

voir le programme >

Avec la CRISC®, accélérez votre carrière et développez votre compréhension de l'impact des risques liés aux SI

La certification CRISC (Certified in Risk and Information Systems), axée autour de la gestion des risques et de la maîtrise des systèmes d'information s'appuie principalement sur les enjeux de gestion globale des risques et également sur des principes de gouvernance et de contrôles des systèmes d'information. La certification CRISC apporte de solides connaissances reconnues à l'échelle internationale sur les enjeux actuels de maîtrise globale des risques informatiques.

Préparation à la certification CRISC®

Objectifs

- Démontrer votre maîtrise de l'ensemble des méthodes et pratiques de gestion des risques conformes à la certification CRISC
- Acquérir le vocabulaire et les principes de l'examen de certification CRISC
- Savoir mettre en œuvre un plan de suivi et de contrôle des risques associés aux systèmes d'information
- Avoir des connaissances avancées dans la gestion des risques en entreprise
- Prouver votre expertise dans l'identification, l'évaluation, la réponse et la surveillance des risques associés aux systèmes d'information
- Savoir concevoir, surveiller et maintenir des contrôles et des solutions basés sur les technologies de l'information pour atténuer les risques

voir le programme >

ISO 27001

Management de la Sécurité de l'Information

La certification ISO/CEI 27001 atteste que vous avez :

- Obtenu l'expertise nécessaire pour aider une organisation à mettre en œuvre un système de management de la sécurité de l'information, conforme à la norme ISO/CEI 27001
- Acquis une compréhension du processus de mise en œuvre du système de management de la sécurité de l'information
- Acquis les connaissances pour prévenir et évaluer les menaces au sein de votre organisation
- Assimiler les connaissances nécessaires afin d'avoir les meilleures chances d'être engagé dans une carrière en sécurité informatique
- Compris le processus de management des risques, des mesures de sécurité et des obligations de conformité
- Acquis les compétences nécessaires pour gérer une équipe chargée de mettre en œuvre un SMSI
- Acquis la capacité à soutenir les organisations dans le processus d'amélioration continue de leur système de management de la sécurité de l'information
- Acquis les compétences nécessaires pour auditer le système de management de la sécurité de l'information de l'organisation

Avec certification

Les cyberattaques sont désormais très récurrentes et les principales cibles des génies de l'informatique mal intentionnés demeurent les grandes entreprises, même si aucune entreprise n'est aujourd'hui épargnée. En mettant en oeuvre un Système de management de la Sécurité de l'Information, vous permettez aux entreprises d'assurer leur développement, grace à la réduction des menaces, et de diffuser une image positive vis-à-vis des clients et des fournisseurs, surtout pour celles possedant des portails de commerce en ligne ou des extranets.

voir le programme >

ISO 27002

Mesure de la Sécurité de l'Information

L'ISO 27002 est une norme internationale qui définit les lignes directrices relatives aux bonnes pratiques de management de la sécurité de l'information. Ces lignes directrices vous servent de feuille de route et vous aident dans la gestion de la sécurité de l'information de vos organisations à renforcer la confiance de vos activités inter-organisationnelles et à mettre en place un ensemble approprié de mesures : les politiques, les processus, les structures organisationnelles et les fonctions logicielles et matérielles. La certification ISO 27002 démontre vos capacités et techniques nécessaires pour la mise en oeuvre et la gestion efficace d'un Système de Management de la Sécurité de l'Information (SMSI) conformément à la norme ISO 27002.

En devenant un professionnel certifié ISO 27002 – vous démontrez que vous avez :

- Compris la mise en œuvre des mesures de sécurité de l'information en conformité avec le cadre et les principes de la norme ISO/CEI 27002
- Obtenu les compétences nécessaires pour accompagner une organisation dans la mise en œuvre et la gestion des mesures de sécurité de l'information selon l'ISO/CEI 27002
- Obtenu l'expertise nécessaire pour aider les organisations à améliorer leur position en matière de sécurité de l'information
- Compris la relation entre les différentes composantes des mesures de sécurité de l'information, y compris la responsabilité, la stratégie, l'acquisition, la performance et la conformité
- Acquis la capacité à effectuer une évaluation périodique des risques dans une organisation

Avec certification

voir le programme >

ISO 27005

Gestion des Risques liés à la Sécurité de l'Information

En devenant un professionnel certifié ISO 27005 – vous prouvez que vous êtes capable de :

- Interpréter les exigences de la norme ISO/IEC 27001 dans le cadre d'un programme de management du risque de la sécurité de l'information
- Assurer la gestion des risques en entreprise conformément à la norme ISO/IEC 27005
- 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 réglementaire
- Diriger une équipe de sécurité de l'information et de management du risque

Avec certification

Avec le développement des technologies de l'information, connaître les risques et les mesures de sécurité liés à l'information est d'une importance capitale. La norme ISO 27005 présente un ensemble de pratiques et de lignes directrices pour guider les professionnels et les organisations vers une protection effective et sans faille de l'information. Au cours de cette formation, vous acquerrez également une compréhension approfondie des bonnes pratiques des méthodes d'évaluation des risques.

voir le programme >

METHODE D'APPRECIATION DES RISQUES
MEHARI, EBIOS ET OCTAVE

L'appréciation efficace des risques pour les entreprises peut s'avérer très compliquée pour des néophytes. Néanmoins, avec des méthodes d'évaluation des risques, on peut acquérir les connaissances solides, nécessaires pour identifier un risque avec succès et apprécier son niveau dans une organisation. Parmi ces méthodes on peut citer **MEHARI, EBIOS et OCTAVE.**

- **MEHARI (Methode Harmonisée d'Analyse de Risque)**
  Développée par le Club de la Sécurité des Systèmes d'Information Français (CLUSIF), MEHARI a pour but la maîtrise parfaite d'une réalisation d'analyse des risques de sécurité de l'information basée sur de la théorie et de la pratique. Cette méthode vous donne les connaissances de base des principes fondamentaux de la sécurité de l'information et de la continuité des activités. La méthode MEHARI vous permet d'identifier les enjeux de la Sécurité des SI.

- **EBIOS (Etude des Besoins et Identification des Objectifs de Sécurité)**
  EBIOS fournit la méthode permettant de construire une politique de sécurité en fonction d'une analyse des risques qui repose sur le contexte de l'entreprise et des vulnérabilités liées à son Système d'Information. Elle vous permet d'acquérir les éléments essentiels relatifs à la gestion des risques liés à l'information. Cette méthode possède des caractéristiques uniques qui permettent son usage dans tous les secteurs de la sécurité. EBIOS vous donne les outils nécessaires pour l'identification des risques d'un SI en construction et demeure idéale pour la rédaction de cahiers des charges.

- **OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)**
  La méthode OCTAVE a pour but de permettre à une entreprise de réaliser par elle-même l'analyse des risques de son Système d'Information. Elle fournit les connaissances et les compétences nécessaires à une exécution optimale de l'évaluation des risques de sécurité ainsi qu'à une gestion opportune des risques en vous familiarisant avec le cycle de vie de ces risques. Cette méthode se base sur des exercices pratiques et des études de cas, permettant de faire une étude complète des risques des organisations.

ISO 27032

Lead Cybersecurity Manager

En devenant un professionnel certifié ISO 27032, vous êtes apte à :

- Connaître les composants et les opérations d'un programme de cybersécurité en conformité avec la norme ISO 27032
- Maîtriser les concepts, méthodes, normes et techniques pour gérer un programme de cybersécurité
- Expliquer l'objectif, le contenu et la corrélation entre l'ISO 27032 et d'autres normes et référentiels
- Piloter un programme de cybersécurité tel que spécifié dans la norme ISO 27032

Avec certification

Les serveurs et ordinateurs de la planète sont quasiment tous interconnectés à travers le réseau internet, une architecture complexe qui évolue à chaque instant .
Face à ces potentielles menaces venant de l'extérieur, les organisations doivent réduire ou annihiler sérieusement leurs risques, tout en minimisant les coûts et les contraintes . La norme ISO 27032 Lead Cybersecurity Manager vous permet d'acquérir une connaissance approfondie de la cybersécurité, de la relation entre la cybersécurité et les autres types de sécurité informatique. Elle encadre et définit la protection et la viabilité à long terme des processus d'affaires dans le cyberespace ainsi que celles des infrastructures informatiques essentielles.

voir le programme >

ISO 27034

Sécurité des Applications

La norme ISO 27034 sécurité des applications a pour objectif de guider les organisations vers une sécurisaton effective de leurs applications, afin de protéger leurs systèmes d'information. Cette formation vous apprendra à connaître la norme ISO/CEI 27034, à comprendre les fondamentaux et techniques nécessaires à la mise en place d'un projet puis, à maîtriser l'application totale de la norme au sein de votre organisation. Elle vous prépare également à l'examen de certification PECB ISO 27034, qui certifie la qualité de votre expertise dans la sécurité des applications.

En devenant un professionnel certifié ISO 27034 – vous êtes apte à :

- Connaître les principes fondamentaux de la sécurité des applications et leurs relations avec les autres normes de sécurité de l'information
- Apprendre les bonnes pratiques, les concepts et techniques pour appliquer les directives de sécurité dans une organisation
- Développer les connaissances nécessaires-pour fournir les meilleures pratiques de sécurité d'application au sein d'une organisation
- Comprendre le rôle et les exigences de chacune des parties prenantes de l'organisation
- Acquérir des compétences professionnelles pour gérer un projet de mise en œuvre de la sécurité des applications

voir le programme >

Avec certification

ISO 27035

Gestion des Incidents de Sécurité de l'Information

En devenant un professionnel certifié ISO 27035 - vous êtes apte à :

- Comprendre les concepts, les approches et les outils pour une gestion efficace des incidents de sécurité de l'information
- Éliminer toute interruption possible et les impacts négatifs sur les opérations commerciales
- Apprendre les techniques les plus avancées pour réagir correctement et efficacement face aux incidents de sécurité de l'information
- Améliorer vos compétences en gestion de la sécurité de l'information et votre analyse des processus d'incidents
- Acquérir les connaissances nécessaires pour mettre en place et piloter une équipe de gestion des incidents de sécurité de l'information
- Obtenir des connaissances sur les bonnes pratiques de gestion de la sécurité de l'information

Avec certification

L'actualité montre que la sécurité de l'information concernant les données en entreprise est un sujet majeur. Les menaces pesant sur les systèmes d'information peuvent engendrer des incidents extrêmement nuisibles pour le fonctionnement et l'image d'une organisation. Pour y faire face, l'Organisation Internationale de Normalisation (ISO) a mis en place la norme ISO 27035:2016 dont le but est de présenter les meilleures pratiques et techniques en gestion des incidents de sécurité.

voir le programme >

ISO 27701

Management de la Protection de la Vie Privée

En devenant certifié ISO 27701 – vous démontrez votre aptitude à :

- Comprendre le processus de mise en œuvre du système de management de la protection de la vie privée
- Soutenir le processus d'amélioration continue du système de management de la protection de la vie privée dans les organisations
- Construire la confiance du client
- Augmenter la transparence des processus et procédures de l'organisation
- Aider une organisation à mettre en œuvre un système de management de la protection de la vie privée conforme à la norme ISO/IEC 27701
- Protéger la réputation de l'organisation

  Augmenter la satisfaction de la clientèle
- Maintenir l'intégrité des informations des clients et des autres parties intéressées

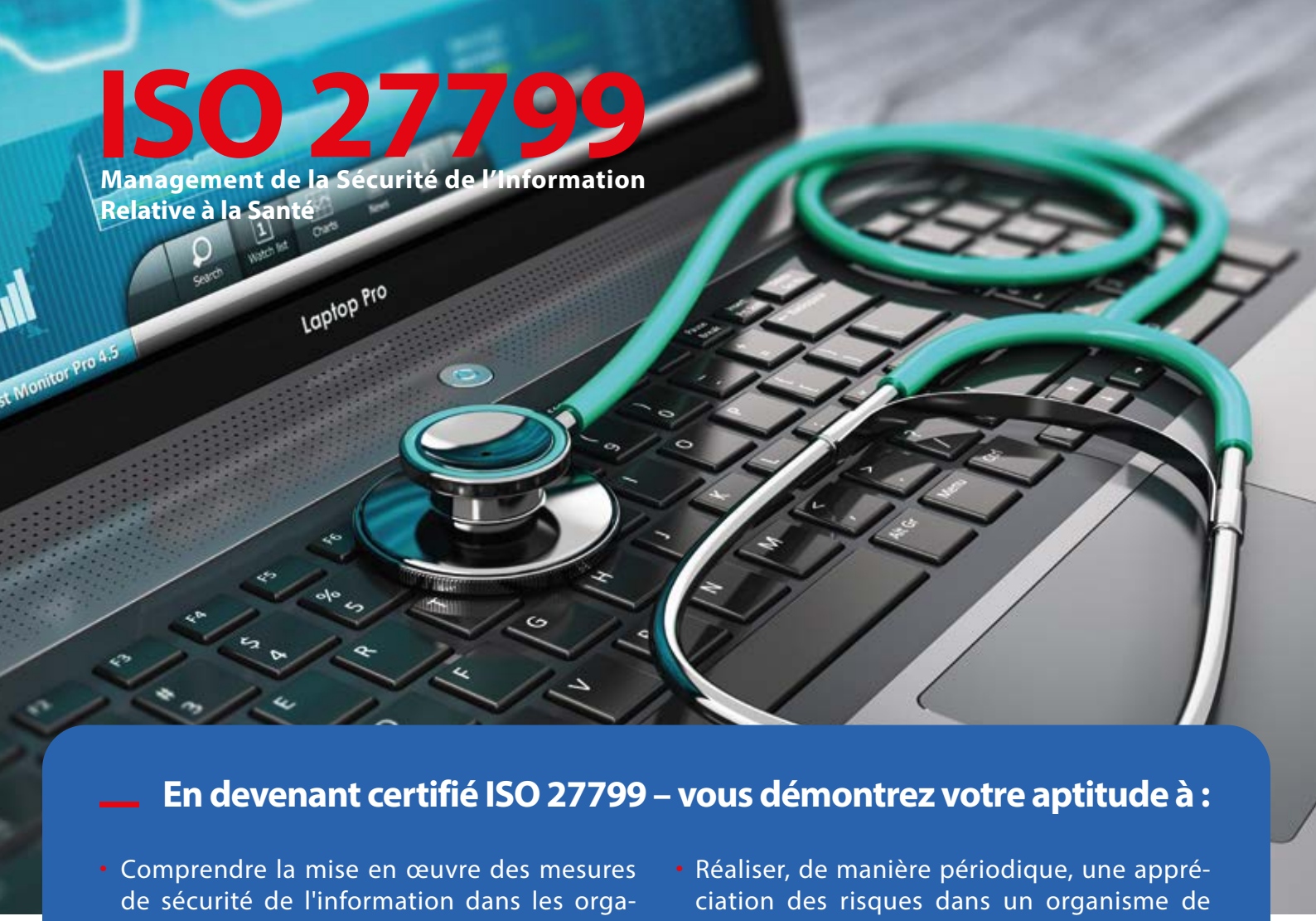
Avec certification

La norme ISO/CEI 27701 est une nouvelle spécification publiée en 2019 qui vise à compléter et à étendre les normes ISO 27001 et ISO 27002. Ce sont les principales normes relatives à la protection des données personnelles dans le cadre de la réglementation de la protection des données (RGPD en Europe et GRPD au Royaume-Uni et dans d'autres pays).
Conçue autour d'une série de cours théoriques et d'exercices pratiques, cette formation vous offre en outre une meilleure compréhension des techniques de gestion des données personnelles et des moyens à mettre en œuvre par votre organisation pour sa mise en conformité avec les textes règlementaires en vigueur

voir le programme >

ISO 27799

Management de la Sécurité de l'Information Relative à la Santé



En devenant certifié ISO 27799 – vous démontrez votre aptitude à :

- Comprendre la mise en œuvre des mesures de sécurité de l'information dans les organismes de santé conforme au cadre et aux principes de l'ISO 27799
- Comprendre la relation entre les différents éléments de mesure de sécurité de l'information, y compris la responsabilité, la stratégie, l'acquisition, la performance, la conformité et le comportement humain
- Soutenir un organisme de santé dans la mise en œuvre et la gestion des mesures de sécurité de l'information en conformité à l'ISO 27799
- Réaliser, de manière périodique, une appréciation des risques dans un organisme de santé
- Aider les organismes de santé à jouer un rôle actif et important dans la protection des données personnelles de leurs patients
- Améliorer la sécurité de l'information au sein des organismes de santé

Avec certification

La norme ISO 27799 décrit sous forme d'exigences et de lignes directrices des méthodes et pratiques vous permettant d'accompagner un organisme de santé dans la mise en oeuvre et la gestion des mesures de sécurité de l'information en conformité avec les normes ISO 27799 et ISO 27002. Cette formation vous donne l'expertise nécessaire en matière de politique de sécurité de l'information, et aussi comment améliorer des politiques déjà existantes au sein d'un organisme de santé. Cette formation vous prépare aussi à l'examen de certification ISO 27799 qui démontre que vous disposez des connaissances pratiques et des capacités professionnelles requises pour accompagner la mise en oeuvre et la gestion des mesures de la sécurité de l'information dans un établissement de santé.

voir le programme >

Oo2 Formations
& Consulting

Audit & Sécurité Informatique

Formations et certifications internationales

Contactez nous !

France

128 rue de la Boétie
75008 Paris

Tel : +33(0) 188 24 70 33
+33(0) 188 24 70 34
Email : contact@oo2.fr

Sénégal

4313 Allées Seydou Nourou Tall
Point E, Immeuble 713, 2 ème étage
BP 45617 Dakar

Tel : +221 33 825 45 54
+221 33 825 72 34
Email : contact@oo2.sn

Côte d'Ivoire

Bd VGE - Marcory
Immeuble Le Massaï
1163 Abidjan 27

Tel : +225 27 225 03 445
+225 27 215 92 870
Email : contact@oo2.ci

Burkina Faso

Avenue du Dr Kwamé
N'Krumah Ouagadougou 01
BP 513

Tel : +226 55 77 87 11
+226 55 79 11 42
Email : contact@oo2.fr

Bénin

Quartier Fidjrossè Fiyégnon 2
Cotonou, Bénin

Tel : +229 69 25 89 89
Email : contact@oo2.bj

www.oo2.fr