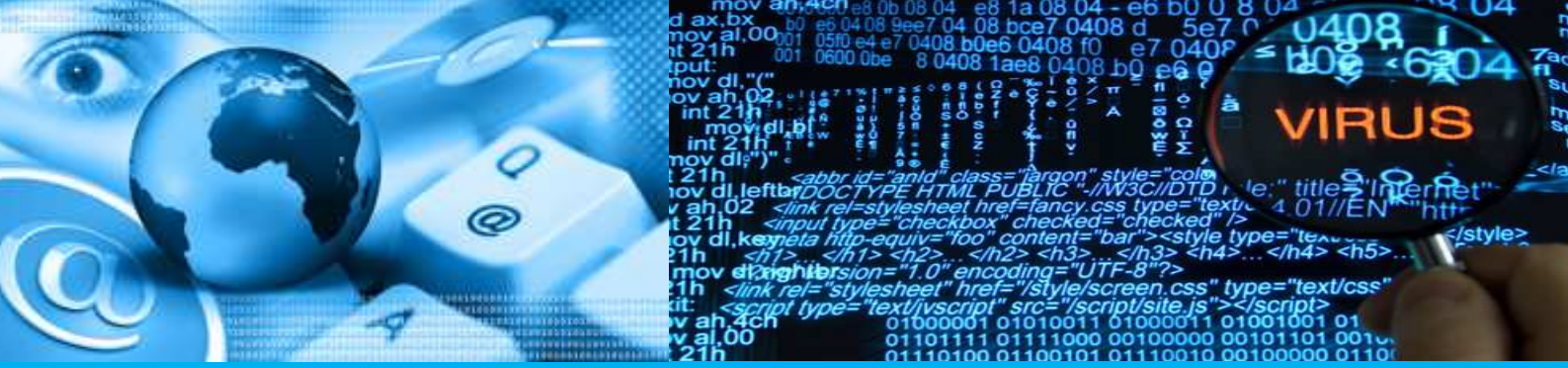


TIC ET SYSTEME D'INFORMATION

A qui s'adressent les formations ?

- *Directeur des systèmes d'information*
- *Responsable des systèmes d'information*
- *Responsable de la sécurité*
- *Responsable de la conformité*
- *Auditeur informatique*
- *Chef de projet informatique*
- *Toutes personnes souhaitent valider leurs acquis par une certification professionnelle reconnue à l'échelle internationale*

L'ISACA (Information Systems Audit and Control Association) est une association internationale regroupant plus de 100'000 membres concernés par les systèmes d'informations de plus de 180 pays.
En s'appuyant sur les connaissances et l'expérience de ses membres, **l'ISACA** a développé des modèles et des pratiques dans les domaines de l'audit des systèmes d'information, de la gouvernance des systèmes d'information, du management de la sécurité et des risques. Les certifications de l'ISACA sont mondialement reconnues et apportent à l'entreprise une réelle valeur ajoutée.

ISACA

- Certified Information Security Auditor **CISA**
- Certified Information Security Manager **CISM**
- Certified in the Governance of Enterprise IT **CGEIT**
- Certified in Risk and Information Systems Control **CRISC**
- Control Objectives for Information and related Technology **COBIT 5**
- Cybersecurity Nexus **CSX**

Certified Information Security Auditor

L'objectif de la formation :

Acquérir et maîtriser les connaissances et les concepts de base de l'audit des systèmes d'information liés à la conception et à la gestion.
Auditer, évaluer, superviser et contrôler selon les exigences de son système d'information

Acquérir les connaissances nécessaires pour conseiller une organisation sur les meilleures pratiques en audit des SI.

Certified Information Security Manager

CISM offre la possibilité aux gestionnaires de la sécurité IT de prouver leurs connaissances et de démontrer leur expertise par un certificat unique défini par **l'ISACA** .Cette certification s'adresse aux responsables de la sécurité des systèmes d'information et aux consultants en sécurité désireux de démontrer leurs expériences et compétences dans le domaine de la sécurité. Elle se différencie des autres certifications sécurité existantes par le fait qu'il s'agit d'une certification sur le management de la sécurité des systèmes d'information et non sur des compétences strictement techniques.

L'objectif de la formation :

- ✓ Gouvernance de la sécurité de l'information
- ✓ Gestion des risques et de la conformité des informations
- ✓ Développement et gestion de programmes de sécurité de l'information
- ✓ Gestion des incidents de sécurité de l'information

Certified in Risk and Information Systems Control

CRISC s'adresse aux professionnels actifs dans la gestion et la prévention des risques, ainsi que dans la définition, la mise en œuvre, le management et la maintenance des contrôles nécessaires pour limiter les risques liés aux systèmes d'information. La désignation CRISC ne permet pas seulement de certifier les professionnels qui ont les connaissances et l'expérience dans l'identification et l'évaluation des risques spécifiques d'une entité, mais également d'aider les entreprises à accomplir leurs objectifs d'affaires dans la conception, la mise en œuvre, la surveillance de contrôles des SI de façon efficace et efficiente.

L'objectif de la formation :

- ✓ Avoir une vision structurée et complète de l'approche orientée risque liée aux systèmes d'information proposée par ISACA en termes d'organisation, de processus et de technologie Identifier, apprécier et évaluer les risques pour permettre l'exécution de la stratégie de management des risques de l'entreprise.

- ✓ Développer et implémenter des réponses aux risques pour minimiser les conséquences d'un éventuel accident et assurer les objectifs métiers.
- ✓ Surveiller les risques et informer les parties prenantes pour assurer la stratégie de management des risques de l'entreprise.
- ✓ Concevoir et mettre en place des contrôles liés aux TIC basés sur les risques métiers pour soutenir les objectifs métiers surveiller et maintenir les contrôles liés aux TIC pour s'assurer qu'ils fonctionnent de manière effective et efficiente.

Certified in the Governance of Enterprise IT

L'objectif de la formation :

Connaître le modèle de la gouvernance IT proposé par l'ISACA pour s'assurer de la définition et de la mise en œuvre des leaderships, des structures organisationnelles et des processus de gouvernance. Savoir aligner la stratégie informatique à la stratégie métier pour s'assurer de la contribution des services IT à l'optimisation des processus métier. Savoir valoriser les livrables pour s'assurer de la fourniture des solutions et des services à temps et au prix convenu.
Savoir manager les risques pour s'assurer de l'existence d'un cadre approprié de gestion des risques et de son alignement aux standards appropriés. Savoir manager les ressources pour s'assurer de la capacité suffisante en ressources de l'IT pour exécuter les tâches courantes et futures . Savoir mesurer les performances pour s'assurer de l'adéquation de la contribution des objectifs IT aux objectifs des métiers de l'entreprise.

Cybersecurity Nexus

CSX s'inscrit dans le prolongement du cadre des compétences requises à l'ère de l'information (SFIA pour Skills Framework for the Information Age) et de l'initiative nationale pour la formation à la cybersécurité (NICE pour National Initiative for Cybersecurity Education). Le certificat teste les connaissances fondamentales en matière de cybersécurité dans cinq domaines :

- ➢ Concepts de cybersécurité
- ➢ Principes de l'architecture de cybersécurité
- ➢ Cybersécurité des réseaux, des systèmes, des applications et des données
- ➢ Réponse aux incidents
- ➢ Sécurité de la technologie en constante évolution

ISC- International Information Systems Security Certification Consortium a été le premier organisme de certification de la sécurité de l'information qui répondre aux exigences de la norme ANSI / ISO / IEC 17024, une référence mondiale pour la certification du personnel. À ce jour, la PAC, CSSLP, SSCP, CISSP ,…et les concentrations de CISSP ont été accrédités selon cette norme, ce qui rend les informations d'identification de (ISC) un must-have chez les professionnels et les employeurs.

ISC

- **CISSP® - Certified Information Systems Security Professional**
- **SSCP® - Systems Security Certified Practitioner**
- **CCFP℠ - Certified Cyber Forensics Professional**

Certified Information Systems Security Professional

A qui s'adresse la formation ?

- ✓ Responsables sécurité du S.I
- ✓ Consultants en sécurité des réseaux et SI
- ✓ Ingénieurs / Techniciens en informatique
- ✓ Administrateurs systèmes & réseaux
- ✓ Administrateur ou ingénieur sécurité
- ✓ RSSI, DSI
- ✓ MCSA, MCSE, CCNP, CCNA
- ✓ et toute personne sensible à l'intégrité de son réseau

Options

Contrôle d'accès.
Sécurité des réseaux et des télécommunications.
Gouvernance de la sécurité et gestion des risques.
Sécurité des développements.
Cryptographie.
Modèles et architectures de sécurité.
Sécurité des opérations.
Continuité des activités et secours informatique.
Aspects légaux, réglementaires, investigations et conformité.
Sécurité physique et environnementale.

Certified Cyber Forensics Professional

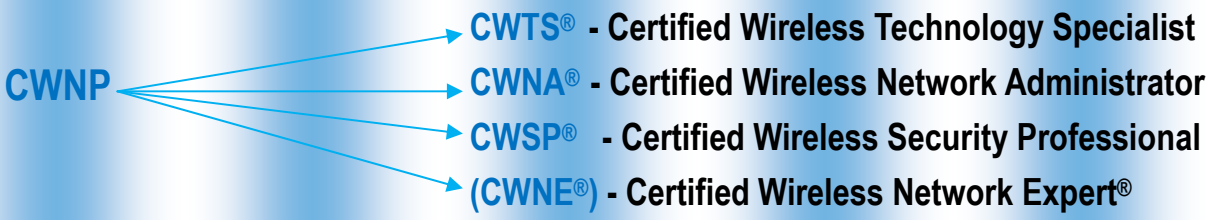
La certification **CCFP** démontre votre expertise dans les techniques et les procédures judiciaires. Avec vos connaissances, vous serez en mesure de présenter des preuves numériques complètes et fiables recevable devant un tribunal de droit.
La certification indique également votre capacité à appliquer l'investegation à l'e-discovery, l'analyse des programmes malveillants et la réponse aux incidents. En suivant cette formation « **CCFP** », vous aurez une expérience pratique sur le déroulement de l'investigation et l'analyse des éléments de preuve de la prise en contact jusqu'à la préparation du rapport finale

Les grandes lignes

- ✓ **Principes juridiques et éthiques** : Ce domaine porte sur le comportement éthique et le respect des cadres réglementaires.
- ✓ **Enquêtes**: Ce domaine englobe les mesures d'enquête et les techniques nécessaires à la collecte des preuves numériques
- ✓ **Forensic Science :** Ce domaine consiste à appliquer un large éventail de sciences et technologies pour enquêter et établir les faits en relation avec le droit pénal ou civil
- ✓ **digital Forensics :** Ce domaine fait référence à la collecte d'éléments de preuve numérique qui peut être défini comme données stockées ou transmises par des moyens électroniques.
- ✓ **Application du Forensics :** Ce domaine porte sur les complexités de criminalité et les types d'applications
- ✓ **Hybrid and Emerging Technologies :** Ce domaine contient les technologies d'évolution que le candidat sera censé comprendre.

CWNP - Certified Wireless Network Professional est un organisme indépendant reconnu comme étant le standard de l'industrie pour la formation et la certification aux réseaux WLAN.
Le cursus de formation proposé fournit aux professionnels réseaux une base complète de connaissances pour progresser rapidement sur la technologie Wireless. De la théorie de base radio aux processus d'échanges des trames 802.11 mais aussi des connaissances pratiques de sécurité requises pour la configuration des réseaux WLAN, ce cours agrémenté d'une série de labs a pour objectif :

- ✓ D'accompagner les stagiaires vers les certifications de maitrise et de performance
- ✓ De permettre aux stagiaires d'acquérir le savoir faire nécessaire pour la mise en œuvre et la gestion des systèmes de sécurité sans fil de l'entreprise, en créant des solutions software et hardware de niveau 2 et 3, avec des outils provenant des fabricants leaders sur le marché.



Certified Wireless Technology Specialist

certification en technologie sans fil **(CWTS),** couvrant les objectifs et les connaissance des fondamentaux de comportement RF, elle décrire les caractéristiques et les fonctions sans fil de composants, et possèdent les compétences nécessaires pour installer et configurer les composants sans fil de matériel de réseau.
Un typique candidat doit avoir une compréhension de base des concepts de réseaux de données.
Les domaines de la formation sont :

- ✓ Wi-Fi Technology, Standards, and Certifications
- ✓ Hardware and Software
- ✓ Radio Frequency (RF) Fundamentals
- ✓ Site Surveying and Installation
- ✓ Applications, Support, and Troubleshooting
- ✓ Security & Compliance

Certified Wireless Network Administrator

A qui s'adresse la formation ?

- Administrateurs: Réseaux, systèmes, infrastructure, sécurité, LAN/WLANS
- Support professionnels
- Designers: Réseaux, systèmes, and infrastructure
- Développeurs: Produits wireless
- Consultants et intégrateurs: IT et sécurité
- Décideurs infrastructure managers, IT managers, directeur de sécurité .CSO , CTO,CCNAS

Objectifs

La formation consiste à passer en revue de manière intensive et systématique toutes les tâches devant être connues par un candidat à la certification **CWNA**. Durant cette phase les aspects importants pour l'examen sont abordés tel que :

- ✓ Radio frequency properties, behaviors, and regulations, and how they affect networking
- ✓ Wireless standards, including 802.11 X
- ✓ General troubleshooting tips to common real-world 802.11n issues
- ✓ General parameters for performing a successful site survey, along with software tools that reduce time and expense
- ✓ Device-level Wi-Fi communications processes
- ✓ Why 802.11n networks operate the way they do and how to apply that knowledge when faced with problems that stump most network administrators
- ✓ Using wireless network analyzers to capture live data and pinpoint potential network issues
- ✓ How using radio frequency makes wireless networks vulnerable
- ✓ Most common wireless threats and how to detect and defend against them
- ✓ Etc ….

Certified Wireless Security Professional

A qui s'adresse la formation ?

- Touts professionnels Sans fil qui cherchent à acquérir une expertise de sécurité sans fil de et en se certifie

Conditions préalables

- ❑ Connaissances solides de réseautage IP
- ❑ Certification CWNA

Objectifs

CWSP certification est une certification LAN sans fil de niveau professionnel.
Obtenir la certification CWSP confirme que vous avez les compétences pour réussir Secure Enterprise réseaux Wi-Fi des pirates, Vous allez couvrir

- Techniques de découverte WLAN
- Techniques d'intrusion et d'attaque
- Analyse de protocole 802.11
- Systèmes de prévention des intrusions sans fil (WIPS) mise en œuvre
- Couche 2 et 3 VPN utilisés en 802.11
- Modèles de conception de sécurité
- Enterprise / SMB / SOHO / réseau public
- Les systèmes sécurité des terminaux
- L'authentification 802.11 et des protocoles de gestion des clés
- Enterprise / SMB / SOHO / réseau public mise en œuvre de solutions de sécurité
- Bâtir des réseaux de sécurité robustes.
- Rapide transition BSS techniques
- Une couverture complète de tous les types 802.1X / EAP utilisé dans les WLAN
- Systèmes de gestion LAN sans fil
- Modèles de conception d'infrastructure d'authentification
- Utilisation des applications sécurisées
  802,11 architectures de conception
- La mise en œuvre d'une politique complète de sécurité sans fil

Certified Wireless Network Expert

La formation consistent à passer en revue de manière intensive et systématique toutes les tâches devant être connues par un candidat à la certification CWNE.
À l'issue de ce cours, vous serez en mesure de:

- ✓ Comprendre et appliquer les concepts essentiels de Fréquence Radio (RF), y compris la planification RF, calculs liés RF et technologies à étalement de spectre.
- ✓ Comprendre le fonctionnement fondamental de réseaux locaux sans fil, d'analyse et de dépannage efficace de problème de WLAN.
- ✓ Analyser et résoudre les problèmes, y compris WLAN couverture RF, multiples, noeuds cachés et les problèmes d'interférence. Travailler avec des outils de diagnostic sophistiqués de WLAN AirMagnet, TamoSoft et plus encore.
- ✓ Comprendre les insécurités dans IEEE 802.11 WLAN.
- ✓ Identifier les attaques qui peuvent se produire contre les pirates du réseau.
- ✓ Sécuriser la transmission de données sur un réseau local sans fil en utilisant le Wi-Fi Protected Access (WPA). ….

Global Information Assurance Certification(GIAC) est le fournisseur et développeur leader de Cyber Certifications sécurité. **GIAC** teste et valide la capacité des praticiens en sécurité de l'information, l'investigation, et de la sécurité du logiciel. les détenteurs de certification GIAC sont reconnus comme des experts dans l'industrie des TI et sont recherchés à l'échelle mondiale par **le gouvernement, l'industrie militaire** et de protéger l'environnement de cyber.

GIAC

- **Global Information Security Fundamentals (GISF)**
- **Global Certified Intrusion Analyst (GCIA)**
- **Global Mobile Device Security Analyst (GMOB)**
- **Global Certified Forensic Examiner (GCFE)**

Global Information Security Fundamentals

Maîtriser

- ✓ Les attaques et contre-mesures
- ✓ Politiques de sécurité du bâtiment
- ✓ Cryptosystems, la cryptographie et algorithmes
- ✓ Défense en profondeur
- ✓ Conception et exécution Réseaux
- ✓ Fondamentaux Concepts de sécurité
- ✓ Mise en réseau et de routage Concepts
- ✓ Risk & Vulnerability Assessment & Management
- ✓ Sécurité en tant que processus
- ✓ Technologies sans fil

Global Certified Intrusion Analyst

Le Cours de certification **GCIA** est conçu pour les professionnels de l'informatique qui travaillent avec les systèmes de détection d'intrusion. Le cours permet aux experts de travailler sur ces systèmes et la façon de configurer les systèmes d'intrusion différents. Lire et interpréter différents fichiers journaux. Quels sont les thèmes abordés par le GCIA de cours, analyste GIAC Certified Intrusion? Les sujets couverts par l'AIPG de cours de certification sont :

- Démonstration de différentes méthodes de réglage IDS
- Accord sur les questions de corrélation
- Analyse des SMTP, HTTP et Microsoft protocoles d'application
- Concepts concernant les communications des IP et TCP
- Comprendre ce qui concerne le fonctionnement de DNS
- Travail de fragmentation
- Compréhension de l'architecture de système anti-intrusion et de son déploiement initial

A qui s'adresse la formation ?

- ❖ Les experts ayant une connaissance en matière de systèmes de détection d'intrusion
- ❖ Toutes personnes souhaitent valider leurs acquis par une certification professionnelle reconnue à l'échelle internationale

Global Mobile Device Security Analyst

La certification GIAC **Mobile Security Device analyste** (**GMOB**) est idéal pour le personnel de sécurité dont le travail et les fonctions consistent à évaluer les appareils mobiles pour trouver des failles de sécurité. Un candidat de GMOB aura une connaissance technique à jour et la compréhension approfondie des tests de pénétration de l'appareil mobile et la capacité d'effectuer une analyse de sécurité de base des applications mobiles. Ils seront également en mesure de comprendre et d'appliquer des politiques de sécurité dans un environnement mobile ainsi que:

- ✓ Testez et atténuer les vulnérabilités
- ✓ Se familiariser avec l'architecture de l'appareil mobile, systèmes d'exploitation, et des fonctions de sécurité.
- ✓ Comprendre les méthodes communes générales utilisées pour attaquer les appareils mobiles, y compris jailbreaking, enracinement, sidejacking, et les attaques d'applications web.
- ✓ Utiliser des techniques communes pour protéger les appareils mobiles, y compris la gestion de configuration et le cryptage..

Global Certified Forensic Examiner

La certification **GCFE** est pour les professionnelles ou intéressés par les industries de la sécurité de l'information, juridiques et d'application de la loi avec un besoin de comprendre l'analyse investigations légales de l'ordinateur. La certification porte sur les compétences de base nécessaires pour recueillir et analyser les données provenant des systèmes d'ordinateurs.
Le GCFE certifie que les candidats possèdent les connaissances, les compétences et la capacité :

- ✓ de mener des enquêtes typiques d'incidents, y compris e-Discovery, analyse médico-légale et de reporting,
- ✓ d'acquisition de données, l'investigation légale de navigateur et de traçage des activités des utilisateurs et des applications sur les systèmes Windows.
- ✓ D'acquérir et examiner les indices de systèmes numériques pour trouver et récupérer des artefacts essentiels connus pour prouver ou réfuter un fait afin de produire un rapport officiel ou la présentation qui pourrait être utilisé en interne ou en litige civil / criminel.

Découvrez comment **mettre en œuvre et améliorer vos processus informatiques, les avantages et les défis à relever grâce à la formation ITIL.** Vous maîtriserez ainsi les cinq grands livres d'**ITIL version 2011** et pourrez ensuite organiser votre département informatique de manière plus efficace et efficiente. Vous apprendrez notamment comment mettre en œuvre les processus ITIL, en vous appuyant sur l'expérience de nos formateurs. Cette formation présente une nouvelle approche de la gestion des services informatiques, des processus et des fonctions innovants, et une évolution des processus existants.
A l'issue de la formation ITIL 2011, les participants seront capables de :

- ✓ Décrire le cycle de vie de la gestion des services à travers les processus clés d'ITIL
- ✓ Décrire les avantages de la mise en œuvre des processus ITIL
- ✓ Décrire relations et interactions entre les processus ITIL
- ✓ Décrire les facteurs clés de succès pour une mise en œuvre performante des processus ITIL

PRINCE2® s'applique à tout type de projet, elle est facilement adaptable. Cette formation vous apportera une connaissance détaillé de tous les concepts de la méthode trois techniques indispensables à une gestion de projet efficace Méthodologie est adoptée par la communauté européenne Londres, Port de Rotterdam,...).
Basé sur des retours d'expérience pluridisciplinaires, dans le domaine informatique PRINCE2, permet d'intégrer parfaitement des méthodes de développement de logiciels de type AGILE, niveau de gouvernance. Les domaines couverts par cette certification sont les suivants :

✓ **Les Themes PRINCE2**

· Cas D'affaire, Organisation, Qualité, Plans
· Risque, Changements, Progression …

✓ **Les Processus PRINCE2**

· Elaborer le Projet, Diriger le Projet, Initialiser le Projet , Contrôler une Séquence de Projet
· Gérer la livraison, Gérer une Limite , Clore le Projet

✓ **Les Techniques PRINCE2**

· Planification basée sur le produit
· Technique de maîtrise des changements
· Technique de revue qualité

A qui s'adresse la formation ?

- **.** DSI
- · Project Management Officer (PMO)
- · Experts fonctionnels ou
- · Consultants IT (AMOA, AMOE)
- · Responsables qualité et gestionnaires des risques

Gestion de Programmes réussis (MSP® - Managing Successful Programmes) a été développé comme un guide de bonnes pratiques en gestion de programmes. Il s'articule autour de **Principes** et de **Processus** à utiliser lors de la gestion d'un programme.
MPS propose les meilleures pratiques de gestion de programmes qui ont fait leurs preuves et permettent de délivrer avec succès les changements transformationnels. Le guide MSP est très flexible et a été conçu pour s'adapter aux besoins spécifiques de chaque organisation. **Cadre de référence MSP (framework)** Le cadre de référence MSP s'appuie sur trois concepts essentiels :

Les principes MSP issus des enseignements (positifs et négatifs) tirés des expériences sur les programmes. Ce sont les éléments communs qui constituent les moteurs de la réussite de tout changement transactionnel, **Les thèmes de gouvernance MSP** qui définissent l'approche d'une organisation dans le cadre de la gestion de programme. Ils permettent à une organisation de mettre en place les responsables, l'équipe de livraison, les structures d'organisation et les contrôles appropriés afin de maximiser les chances de réussite,

Objectifs

Création de votre propre cycle de vie d'un programme

- Concevoir votre équipe
- Comment les leaders dirigent-ils un programme ?
- Rédaction d'un programme court
- Comment être certain des avantages réalisés avec une bonne gestion du changement
- Engager la communication entre les parties prenantes d'un programme
- Gérer les risques et les problèmes
- S'assurer de la qualité du programme final
- Planifier, Suivre et Contrôler la progression dans le programme
- Présenter une définition du programme
- Gérer le développement de nouveaux Business et contrôler les changements
- Intégrer les processus, l'information et les rôles dans le programme

Processus de gestion du Programme

- Identifier un programme
- Définir un programme
- Diriger un programme
- Gérer les avantages d'un programme
- Terminer un programme