INFORMATION-TECHNOLOGIE-SECURITE

ITS est une entreprise spécialisée dans la sécurité des systèmes d'information, les investigations numériques, l'audit des systèmes d'information et la gouvernance des systèmes d'information.

Le besoins de maitriser le risque dans un système d'information est sans doute lié aux conséquences éventuelles de l'occurrence de la réalisation d'une menace sur les services du système d'information en question. Il est donc indispensable d'anticiper sur toute situation capable de détruire la qualité du service dans un système d'information.

C'est compte tenu de ce constat que nous vous proposons depuis l'année 2008 une gamme de services (Consultations, assistance technique, conseils, conception et développement de systèmes, installations et configurations de ces derniers, ainsi que le renforcement des capacités de vos cadres) dans les domaines lies à la gestion du risque dans vos systèmes d'information.

Nous avons pour cela au sein de notre entreprise une équipe de spécialistes, de managers, d'experts et de chercheurs de hautes compétences pour vous apporter satisfaction dans vos besoins divers en sécurité des systèmes d'information, investigations numériques, audit des systèmes d'information et gouvernance de ces derniers.

En plus de nos compétences internes, nous exploitons un nombre très grands d'experts et consultants internationaux que nous choisissons parmi les grands professeurs d'universités, professionnels d'entreprises et autres pour assurer un excédant d'apport dans les paquets de services que nous vous proposons.

Nous vivons dans un monde ou la compétence est plus que jamais garante du succès et où l'anticipation dans la gestion des situations est la règle d'or pour tout management, ceci est d'autant plus vraie quand on parle de systèmes d'information.

Nous remercions tous ceux qui nous ont fait confiance et continuent de travailler avec nous, et invitons les autres à venir partager avec nous leur problèmes auxquels nous essayerons ensemble de trouver des solutions adaptées au cas par cas.

La cybercriminalité continuera d'évoluer si nous nous ne faisons rien, il est de la responsabilité de tous, chacun à son niveau et pour son bien personnel et ensemble pour le bien de tous de maitriser le risque dans nos systèmes d'information.

BP: 8570 Yaoundé - CAMEROUN
Gsm: (+237) 94 03 14 76 - 79 28 69 31
Tel.: (+237) 22 07 08 06 - 22 07 08 48
Fax: +15817013252
Site Web: www.groupits.cm
Courriel: info@groupits.cm

SECURITE DES SYSTEMES D'INFORMATION

(Consultations, conseils, formations hors ligne et en ligne, conception, développement, assistance techniques, recherche, études et réalisations)

Cryptologie

Virologie Informatique

Audit de sécurité des SI

Analyse de risques informatiques

Management de la sécurité des SI

Normes dans la sécurité des SI

Signature Numérique

Protocoles de sécurité et VPN

Systèmes de payement en ligne

Gestion des attaques du système informatique

Spam et Logiciels espions

Steganographie

Gestion des Incidents Informatiques

BP: 8570 Yaoundé - CAMEROUN
Gsm: (+237) 94 03 14 76- 79 28 69 31
Tel.: (+237) 22 07 08 06- 22 07 08 48
Fax: +15817013252
Site Web: www.groupits.cm
Courriel: info@groupits.cm

SERVICES

Aujourd'hui l'implémentation des technologies de l'information et de la communication engendre les problèmes de types nouveaux de sécurité des informations sensibles, des infrastructures et organisations mises en place. Ainsi le contrôle et la gestion du risque informationnel dans ces nouveaux systèmes deviennent indispensables pour le bon fonctionnement et même l'existence de ces derniers. Les exemples de failles dans les systèmes de sécurité et de protection informatique dans les services d'une entreprise ou organisation peuvent être catastrophiques allant de la saturation des réseaux de communication jusqu'à la destruction totale du système d'information, ce qui très souvent engendre des pertes économiques considérables pour l'entreprise ou l'organisation concernée. Dans le but de mieux gérer les risques et menaces de sécurité sur vos informations et systèmes d'information, i.T.s vous apporte des solutions intelligentes et efficaces de sécurité suivantes :

Consultations, Conseils et Formations pour:

- Veille stratégique aux infections virales ;
- Veille stratégique à l'intrusion des programmes espions ;
- Barrage contre l'intrusion illégale aux ordinateurs et systèmes d'information ;
- Usage des pare-feu et du système de sécurité Windows ;
- Cryptage de l'information ;
- Contrôle des points de vigilance du système d'information ;
- Cryptage et signature numérique ;
- Mesures de sécurité contre le hacking, cracking et phishing;
- Sécurisation des communications électroniques;
- Mise en place des systèmes de management de la sécurité des systèmes d'information;
- Analyse des risques informatiques avec l'usage des normes (MEHARI, EBIOS.....);
- Audits de sécurité des systèmes d'information;
- Maitrise des normes en matière de sécurité des systèmes d'information (ISO 2700X...);
- Contrôle d'accès et gestion des identités numériques;
- Authentification et gestion de l'intégrité des informations, usagers et équipements;
- Sécurisation des transactions électroniques pour le commerce et autres services en ligne;
- Implémentation des protocoles de sécurité (IPSec; SSL/TLS; SSH etc...);
- Réalisation des réseaux privés virtuels;
- Implémentation des certificats numériques pour la sécurisation des services en ligne;
- Récupération des données cachées, cryptées ou effacées;
- Récupération des mots de passe oubliés ;
- Destruction de virus et programmes espions.

SERVICES

L'utilisation des systèmes d'information de plus en plus complexe et leur implémentation dans le contrôle et la gestion des processus sensible imposent une normalisation visant la conformité de tous les systèmes d'information selon l'activité et le métier dans le but de mieux maitriser le risque qu'engendre le système d'information dans le fonctionnement de toute organisation. Ainsi l'audit des systèmes d'information comme activité visant à mesurer le niveau de conformité d'un système d'information par rapport à des règles bien définies et à examiner le niveau de dérive du système par rapport à ces standards aide à anticiper sur les problèmes et à proposer les solutions pour y remédier avant même l'occurrence d'incidents. ITS dans ce sens vous propose les services de :

Consultations, Conseils et Formations pour:

- Processus métier du Système d'information ;
- Analyse et gestion des risques informatiques ;
- Chapitres du COBIT et gestion des processus ;
- Implémentation du COBIT et ITIL dans l'audit des S.I ;
- Usage de MEHARI dans l'étude des risques ;
- Contrôle des services du système d'information ;
- Logiciels d'audit des S.I. (MS Excel ; IDEA Caseware) ;
- Rapports de contrôle et de mission;
- Etapes de l'audit des Systèmes d'information;
- Extraction et analyse des données;
- Echantillonnage statistique des données.....;
- Vérification des données et des processus;
- Contrôle d'applications et d'équipements
- Contrôle d'accès et gestion des privilèges;
- Détection des fraudes
- Détection de fausses écritures dans les bases de données;
- Vérification d'identités..);
- Authentification de données, applications, équipements et processus;
- Détermination de sources et traces de fraudes informatiques
- Récupération des données cachées, cryptées ou effacées;
- Récupération des mots de passe oubliés ;
- Conduite et vérification des recommandations;
- Analyse de données sensibles ;
- Audit des projets informatiques ;
- Risques dans l'audit des S.I. ;
- Contrôles et verification Internes ;
- Contrôles et vérifications généraux ;
- Suivi des corrections d'irrégularités.

AUDIT DES SYSTEMES D'INFORMATION

(Consultations, conseils, formations hors ligne et en ligne, conception, développement, assistance techniques, recherche, études et réalisations)

Méthodologie d'audit des S.I.

Normes dans l'audit des S.I.

COBIT

MEHARI

Risques d'audit des S.I.

Outils d'Audit des S.I.

Rapports d'Audit des S.I.

Bonnes Pratiques en Audit des S.I.

Vérification et contrôle des S.I

Ethique dans l'audit des S.I.

Types d'Audit des S.I.

Limites d'Audits des S.I.

Contrôle des systèmes Informatiques

BP: 8570 Yaoundé - CAMEROUN
Gsm: (+237) 94 03 14 76- 79 28 69 31
Tel.: (+237) 22 07 08 06- 22 07 08 48
Fax: +15817013252
Site Web: www.groupits.cm
Courriel: info@groupits.cm

INVESTIGATIONS NUMERIQUES

(Consultations, conseils, formations hors ligne et en ligne, conception, développement, assistance techniques, recherche, études et réalisations)

Méthodologie d'investigations numériques

Preuve numérique

Surveillance Numérique

Traces d'attaques

Empreinte Numérique

Outils d'investigations numériques

Rapports de garde

Scène numérique du crime

Scelle numérique

Rapport d'investigation

Logiciels d'investigations numériques

Récupération de données cryptées, détruites ou cachées.

Assistance technique auprès des juridictions

BP: 8570 Yaoundé - CAMEROUN
Gsm: (+237) 94 03 14 76- 79 28 69 31
Tel.: (+237) 22 07 08 06- 22 07 08 48
Fax: +15817013252
Site Web: www.groupits.cm
Courriel: info@groupits.cm

SERVICES

La cybercriminalité gagne du terrain avec la globalisation des systèmes d'information et l'intensification de leur utilisation dans tous les domaines d'activités de l'homme. La coopération internationale ne promet pas de résultats intéressants en même temps que les cybercriminels exploitent de mieux en mieux les technologies d'attaques disponible, et ceci dans des conditions de partage d'expériences très bonnes. La police et les services de sécurité trainent le pas même si la législation permettant de combattre le fléau prend corps. La loi ne peut être efficace que si la preuve numérique du crime commis est à la disposition de la justice. C'est pour cette raison que l'investigation numérique qui représente un ensemble de moyens et techniques permettant de trouver, traiter, présenter et protéger l'information preuve numérique d'infractions est le moyen le plus efficace dans la lutte contre la cybercriminalité. Dans le but de vous aider à remonter sur la preuve numérique des infractions, ainsi que sur les traces de leur auteurs ITS vous propose les services de :

Consultations, Conseils et Formations pour:

- Processus et procédures d'investigations numériques ;
- Analyse et gestion des preuves numériques ;
- Récupération d'information des disques, PDA et téléphones portables ;
- Outils de preuves pour mobiles ;
- Surveillance Numérique;
- Cryptanalyse de données extraites ;
- Logiciels d'investigation numérique (Winhex et autres) ;
- Rapports d'investigations numériques;
- Etapes d'une investigation numérique;
- Extraction et analyse des données cachées ou cryptées;
- Protection de la scène du crime numérique.....);
- Vérification des données et des processus;
- Révélé des données sur la scène du crime numérique
- Outils d'extraction de données;
- Détection de preuves numériques
- Détection de traces de crime dans un système d'information;
- Vérification d'identités numériques d'attaquants;
- Remontée sur la preuve et l'identité d'une attaque numérique;
- Détermination de sources d'attaques informatiques
- Usage de réseaux sociaux pour la traque numérique;
- Assistance technique aux procédures contentieuses et précontentieuses;
- Gestion de la preuve numérique;
- Protection de la preuve numérique ;
- Détection de comportement à risque;
- Détection d'attaques et d'intrusions numériques ;
- Prévention d'intrusion et d'attaques numériques ;

SERVICES

GOUVERNANCE DES SYSTEMES D'INFORMATION

(Consultations, conseils, formations hors ligne et en ligne, conception, développement, assistance techniques, recherche, études et réalisations)

Méthodes de gouvernance des S.I.

Normes dans la gouvernance des S.I.

COBIT

ValIT et ITIL

Planification et gestion d'un S.I.

Niveaux de maturité de la gouvernance des S.I.

Bonnes Pratiques en gouvernance des S.I.

Gestion des taches et création de valeurs dans un S.I

Investissements et retour sur investissement dans un S.I.

Mise en œuvre de la gouvernance des S.I.

Outils de gouvernance des S.I.

Toute activité nécessite un système de gouvernance solide et efficace pour s'assurer de la pérennité de cette dernière, ainsi que de l'atteinte des objectifs fixe au départ. Le système d'information ne s'aurait faire exception à cette règle, au contraire nécessite plus d'attention dans ce sens car complexe et indispensable pour toute entreprise. Les investissements fais pour son système d'information doivent se justifier non pas par un besoin simple, mais au moyen d'une étude préalable présentant le gain retour sur cet investissement par la création et l'exploitation des services lies à l'investissement en question. C'est ainsi que la gouvernance du système d'information se trouve au centre de toute entreprise aujourd'hui avec un ensemble de méthodes et normes qui l'accompagne: Pour vous aider à mettre en place un système de gouvernance dans votre système d'information, ITS vous propose :

Consultations, Conseils et Formations pour:

- Processus métier du Système d'information ;
- Gestion des taches pour création de valeur ;
- Usage de la norme ValIT pour la gestion des investissements et le calcul du retour sur investissement dans un système d'information ;
- Implémentation du COBIT et ITIL dans la gouvernance des S.I ;
- Usage de différentes méthodes de gouvernance des S.I. ;
- Fourniture des services dans un système d'information ;
- Evaluation de la maturité d'un système de gouvernance du S.I. ;
- Mise en place et gestion des centres de services informatiques;
- Etapes de la gouvernance du système d'information;
- Outils de gouvernance du S.I;
- Instruments de mesure du niveau de gouvernance des S.I.;
- Amélioration de la gouvernance des S.I.;
- Schéma directeur du système d'information
- Création et amélioration des services du système d'information;
- Certification en gouvernance des S.I. et organismes y lies ;
- Suivi des services et amélioration des résultats;
- Rôles de la gouvernance des S.I.;
- L'importance des référentiels dans les processus de gouvernance des S.I.;
- Détermination des besoins en gouvernance de S.I.
- Eléments de gouvernance des S.I;
- Gestion du changement lie à la mise en place d'un système de gouvernance du S.I. ;
- Conduite des contrôles du système de gouvernance des S.I;
- Choix de techniques et méthodes de gouvernance des S.I. ;
- Audit des fonctions de la gouvernance du S.I;
- Evaluation des apports de la gouvernance du S.I. ;
- ValIT et le calcul du retour sur Investissement dans un S.I.;
- ValIT comme complément au Cobit

BP: 8570 Yaoundé - CAMEROUN
Gsm: (+237) 94 03 14 76- 79 28 69 31
Tel.: (+237) 22 07 08 06- 22 07 08 48
Fax: +15817013252
Site Web: www.groupits.cm
Courriel: info@groupits.cm

PROJETS

ETUDES

AUTRES SERVICES

BP: 8570 Yaoundé - CAMEROUN
Gsm: (+237) 94 03 14 76- 79 28 69 31
Tel.: (+237) 22 07 08 06- 22 07 08 48
Fax: +15817013252
Site Web: www.groupits.cm
Courriel: info@groupits.cm

PROJETS, ETUDES ET AUTRES SERVICES

1. *DEVELOPPEMENT DES NORMES ET STANDARDS EN MATIERE DE SECURITE INFORMATIQUE*
2. *DEVELOPPEMENT D'OUTILS DE SECURISATION DES SITES WEB EN .CM*
3. *DEVELOPPEMENT DES SYSTEMES DE PAYEMENT ELECTRONIQUES*
4. *DEVELOPPEMENT DES SYSTEMES DE COMMERCE ELECTRONIQUE*
5. *DEVELOPPEMENT DU PORTAIL « MARCHE VIRTUEL » WWW.ANNONCES.CM*
6. *DEVELOPPEMENT DU PORTAIL DE PROCEDURE ADMINISTRATIVES « LE CONSULTANT »*
7. *LABVIRTUELS*
8. *REALISATION D'ETUDES SUR L'IMPACT ECONOMIQUE ET GEOSTRATEGIQUE DU RISQUE INFORMATIONNEL AU CAMEROUN*
9. *LE MANAGEMENT DE LA SECURITE DES SYSTEMES D'INFORMATION*
10. *ANALYSE DES RISQUES TI*
11. *PROJETS DE SECURITE EN COLLABORATION AVEC « FUNDACION PUERTOS DE LAS PALMAS »-Valence-Espagne*
12. *DEVELOPPEMENT D'OUTILS D'INVESTIGATIONS NUMERIQUES (EN PARTENARIAT AVEC DECISION GROUP – TAIWAN - http://www.edecision4u.fr)*
13. *DEVELOPPEMENT DES SYSTEMES DE COMMUNICATION SECURISES (EN PARTENARIAT AVEC TECHNICAS COMPETITIVAS – ESPAGNE - http://www.tecnicascompetitivas.com)*
14. *DEVELOPPEMENT DES SYSTEMES D'INFORMATION DE GESTION (EN PARTENARIAT AVEC PRODEVELOP – ESPAGNE- http://prodevelop.es)*
15. *RECUPERATION DES DONNEES (MOTS DE PASSE , CLES ET AUTRES) EFFACEES*
16. *DEVELOPPEMENT ET HEBERGEMENT DE PORTAILS WEB SECURISES*
17. *DEPLOIEMENT DES SYSTEMES BIOMETRIQUES*
18. *IMPLEMENTATION DES SYSTEMES DE CONTROLE D'ACCES*
19. *ETUDES SUR LES SYSTEMES D'INFORMATION*
20. *ASSISTANCE EN GESTION DES RISQUES INFORMATIQUES*

LE CENTRE DE FORMATION DE ITS EST UN CENTRE DE FORMATION DE REFERENCE SPECIALISE DANS LA GESTION DES RISQUES DANS LES SYSTEMES D'INFORMATION AVEC UNE ORIENTATION SUR:

1. ***LA SECURITE DES SYSTEMES D'INFORMATION***
2. ***LES INVESTIGATIONS NUMERIQUES***
3. ***L'AUDIT DES SYSTEMES D'INFORMATION***
4. ***LA GOUVERNANCE DES SYSTEMES D'INFORMATION***

LES FORMATIONS ONT UN CYCLE DE DOUZE MOIS, SOIT NEUF MOIS DE COURS ET TROIS MOIS DE PRATIQUE EN ENTREPRISE. LE CENTRE DE FORMATIONS CF-ITS EST AGREE PAR LE MINEFOP ET DONC DELIVRE LES CERTIFICATS DE FIN DE FORMATION CONFORMEMENT A LA REGLEMENTATION EN VIGUEUR.

EN PLUS LE CENTRE EST AGREE CISCO ACCADEMY, DONC PREPARE AUX CERTIFICATS CISCO.

CF-ITS PREPARE EGALEMENT ET INSCRIT AUX EXAMENS SUR LES QUATRE CERTIFICATS D'ISACA

EN SOMMES, CF-ITS PREPARE AUX CERTIFICATS SUIVANTS :

Certification Professionnelle Nationale (MINEFOP)

Sécurisation des systèmes d'Informations

Investigations numériques

Audit des systèmes d'information

Gouvernance des systèmes d'information

Certification Professionnelle Internationale (ISACA)

CISM - Certified Information Security Manager

CISA - certified Information Systems Auditor

CRISC - Certified in Risk and Information Systems Control

CGEIT-Certified in Governance of Enterprise IT

Certification Professionnelle Internationale (CISCO)

CCNA (Cisco certified network associate)

CCNP & CCNP Security (former CCSP)

CCNA Security

CF-ITS

Centre de formation de ITS

BP: 8570 Yaoundé - CAMEROUN
Gsm: (+237) 94 03 14 76- 79 28 69 31
Tel.: (+237) 22 07 08 06- 22 07 08 48
Fax: +15817013252
Site Web: www.groupits.cm
Courriel: info@groupits.cm

QUELQUES IMAGES

IMAGES DE QUELQUES FORMATIONS

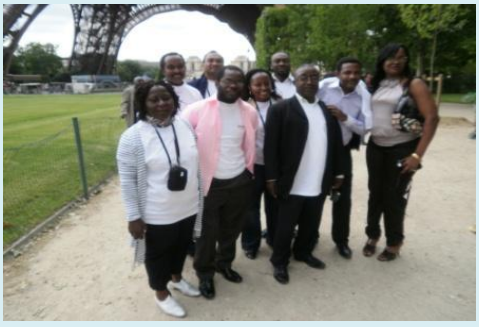
Séminaire de Mars 2011 (KRIBI)

Séminaire de Juin 2012 (KRIBI)

Séminaire d'Aout 2012 (PARIS)

Séminaire de Septembre 2012 (KRIBI)

Séminaire de Novembre 2012 (KRIBI)



BP: 8570 Yaoundé - CAMEROUN
Gsm: (+237) 94 03 14 76- 79 28 69 31
Tel.: (+237) 22 07 08 06- 22 07 08 48
Fax: +15817013252
Site Web: www.groupits.cm
Courriel: info@groupits.cm

SEMINAIRE DE FORMATION

PROTECTION ET SECURITE DES INFORMATIONS STRATEGIQUES

Données de base

Etre un spécialiste du domaine des TIC ;
Un responsable d'entreprise et maitriser l'outil informatique, un spécialiste du domaine de la sécurité (Police, Militaire etc.…), un responsable ou opérateur dans une banque, un Juriste ou associé ; un étudiant dans les TIC

Public cible

Toute personne déjà initiée ou non à la maitrise du risque métier dans un système d'information, à sécuriser ou à accompagner la sécurisation du SI, à définir la politique de sécurité des informations, à travailler avec des informations sécrètes.

Animateurs

Dr. BELL B.G.

° PhD-sciences techniques en méthodes et systèmes de protection de l'information, sécurité des informations ;
° Spécialiste en cryptologie (St. Petersburg) ;
° Expert en sécurité et protection des SI ;
° Enseignant-Chercheur (UCAC,ENSPY,UPAC)
° Directeur de ITS (www.groupits.cm)
° Membre permanent de l'association internationale d'audit et du contrôle des systèmes d'information (**ISACA** : **www.isaca.org**)
° Membre de l'association internationale de recherche en cryptologie (**IACR : www.iacr.org**)

Méthodologie

Pédagogie active, réponses individualisées aux besoins des participants. Exposés théoriques, apports méthodologiques et nombreux travaux pratiques.
Chaque participant est invité à venir exposer ses besoins en sécurité et protection des informations.

Lieu

Kribi

Période

26, 27 et 28 Mars 2013

Durée

3 jours

Coût

900.000 Fcfa/ personne

Tarifs(HT) incluant les frais pédagogiques, les frais de documentation, les frais du matériel de formation et les frais de déjeuner pendant la formation Un ordinateur portable offert à chaque participant

OBJECTIFS – AMENER LES PARTICIPANTS A :

- Comprendre les mécanismes de sécurisation des informations sensibles
- Maitriser les notions et technique de protection de données stratégiques
- Maitriser la gestion et la protection du secret
- Créer et entretenir les conditions d'extrême confidentialité des informations
- Utiliser la cryptologie (science du secret) pour la protection des informations
- Gérer et garantir la confidentialité des informations en situation critique

RESULTATS ATTENDUS – LES PARTICIPANTS MAITRISENT :

- Les technique de protection de la transmission des donnés dans un SI
- Le combat contre la fuite d'informations sensibles
- L'usage de systèmes de cryptage de l'information
- Les méthodes et systèmes de protection et sécurité des informations
- Les risques de fuite et exposition des informations sensibles
- La sensibilité des informations et leur protection

PROGRAMME ET DEROULEMENT DE LA FORMATION

- ***1er Jour : Informations et sensibilité***
  - Qualité et quantité de l'information ;
  - Information ressource ; information stratégique ; information sensible ;
  - Théorie de l'information : concepts, notions, processus et phénomènes y liés ;
  - Systèmes d'information
- ***2ème Jour : sécurité des informations***
  - Risque informationnel ;
  - Gestion du risque informationnel ;
  - Menaces sur l'information, vulnérabilité de l'information et contre-mesures ;
  - Politique générale de sécurité des informations
- ***3ème Jour : protection des informations***
  - Gestion de la sécurité des informations ;
  - Méthodes de protection de l'information ;
  - Systèmes de protection de l'information ;
  - Applications de la cryptologie dans la protection de l'information

Invités

1. **Sergei VOROBEV**, **(Fédération de Russie)**
   - Directeur de ICI PRO
   - Représentant de Kaspersky Labs et Dr WEB en zone CEMAC
2. **Un Juriste**, spécialiste de la protection de l'information et de la cyber sécurité

Programme Culturel

Débats chaque soir sur :

1. Les enjeux stratégiques de la sécurité des informations sensibles : Impacts de la loi sur la cyber sécurité et cybercriminalité
2. Cryptologie (science du secret) : importance stratégique pour la société de l'information et rapports avec la loi
3. Protection de l'information : enjeux économiques et commerce électronique

ITS – BP: 8570, Yaoundé-Cameroun; Web: http://www.groupits.cm;
Tel: (+237) 22070806, 22070848, 94031476, 79286931; Fax: +15817013252
Email: info@groupits.cm

SEMINAIRE DE FORMATION

AUDIT INFORMATIQUE

Données de base

Etre un spécialiste du domaine des TIC ;
Un responsable d'entreprise et maitriser l'outil informatique, un responsable ou contrôleur dans une banque ou PME, un consultant en audit des SI ; un étudiant dans les TIC

Public cible

Toute personne déjà initiée ou non à la gouvernance d'entreprise, amenée à assurer le contrôle et suivi des systèmes d'information d'une entreprise, à assurer la conformité du système d'information.

Animateurs

Yves J. NDJE (Cameroun)
° Enseignant-Chercheur, Université de Douala ;
° Membre du Laboratoire XLIM UMR 6172, Université de Limoges (France) ;
° Equipe de recherche : Sécurité Informatique, Cryptographie et Codage.
° E-mail : yves-jonathan.ndje@xlim.fr

Christelle BIBEE (Cameroun) : Master en Management des systèmes d'information ; consultante à ITS.

Méthodologie

Pédagogie active, réponses individualisées aux besoins des participants. Exposés théoriques, apports méthodologiques et nombreux travaux pratiques.
Chaque participant est invité à venir exposer ses besoins en sécurité et protection des SI.

Lieu

Kribi

Période

23, 24 et 25 Avril 2013

Durée

3 jours

Coût

900.000 Fcfa/ personne

Tarifs(HT) incluant les frais pédagogiques, les frais de documentation, les frais du matériel de formation et les frais de déjeuner pendant la formation. ***Un ordinateur portable offert à chaque participant.***

OBJECTIFS – AMENER LES PARTICIPANTS A :

- Comprendre les objectifs de l'audit informatique ;
- Appréhender la conduite d'une mission d'audit informatique ;
- Comprendre l'audit de la fonction sécurité ;
- Connaître les outils de l'audit informatique ;
- Appréhender la gestion des risques ;
- Comprendre les objectifs du Référentiel CobiT.

RESULTATS ATTENDUS – LES PARTICIPANTS MAITRISENT :

- La démarche de l'audit informatique ;
- Les spécificités de l'audit de projet ;
- L'analyse des données ;
- Les « bonnes pratiques » de CobiT et leur mise en œuvre ;
- La rédaction d'un rapport d'audit informatique ;
- Le code éthique de la profession d'auditeur informatique.

- ***1er Jour : Audit informatique : Introduction***
  - Raison d'être de l'audit informatique ;
  - Champ d'application de l'audit informatique;
  - Méthodologie d'Audit Informatique
- ***2ème Jour : Audit et sécurité***
  - Evaluation des risques ;
  - Audit et la fonction sécurité ;
  - Normes professionnelles de l'Auditeur Informatique
- ***3ème Jour : Outils et Référentiel CobiT***
  - Outils de l'audit informatique ;
  - Audit de projet et processus de CobiT.
  - Applications et cas d'étude d'audit informatique

Invité

1. **Prof. Jean-Robert KALA KAMDJOUG, (Cameroun)**

Professeur à l'Université Catholique d'Afrique Centrale, responsable du Master –Management des Systèmes d'information

Programme culturel

Débats chaque soir sur :

1. L'Audit comme outil de bonne gouvernance dans les S.I
2. La norme et conformité en Audit Informatique
3. Rapports d'Audit informatique et éthique

Visite des chutes de la LOBE

ITS – BP: 8570, Yaoundé-Cameroun; Web: http://www.groupits.cm;
Tel: (+237) 22070806, 22070848, 94031476, 79286931; Fax: +15817013252
Email: info@groupits.cm

SEMINAIRE DE FORMATION

RESEAUX SOCIAUX : ROLES ET USAGES DANS LA STRATEGIE DE SECURITE DES SOCIETES MODERNES

Données de base

Etre un spécialiste du domaine des TIC ;
Un spécialiste du domaine de la sécurité (Police, Militaire etc.…),

Public cible

Toute personne déjà initiée ou non a la recherche de l'information, à créer ou accompagner la création d'opinions, à définir et orienter la politique et les objectifs de la masse sociale, a créer une motivation aux fin d'atteindre les objectifs de décision, a anticiper sur le comportement social pour mieux orienter les politiques de sécurité y liées

Animateurs

1. **Dr. BELL B.G. (Cameroun)**

° PhD-sciences techniques en sécurité et protection des systèmes d'information;
° Spécialiste en cryptologie (St. Petersburg) ;
° Expert en sécurité et protection des SI ;
° Enseignant-Chercheur (UCAC,ENSPY,UPAC)
° Directeur de ITS (www.groupits.cm)

2. **Jerry KATHINGO (Kenya)**

o ISACA, CISM- Commetee Member.
Expert en sécurité et protection des systèmes d'information

Méthodologie

Pédagogie active, réponses individualisées aux besoins des participants. Exposés théoriques, apports méthodologiques et nombreux travaux pratiques.

Chaque participant est invité à venir exposer ses besoins en usage des réseaux sociaux

Lieu

Kribi

Période

22, 23, 24, 25 et 26 Avril 2013

Durée

5 jours

Coût

1200.000 / personne

Tarifs (HT), incluant les frais pédagogiques, les frais de documentation, les frais de matériel de formation et de déjeuner pendant la formation. Un ordinateur portable offert à chaque participant.

OBJECTIFS – AMENER LES PARTICIPANTS A :

- Comprendre les mécanismes de sécurité a l'ère du numérique
- Comprendre l'usage des réseaux sociaux comme arme informationnelle
- Comprendre la désinformation sociale et guerre informationnelles
- Maitriser le phénomène de camouflage social
- Utiliser les réseaux sociaux comme gites informationnelles

RESULTATS ATTENDUS – LES PARTICIPANTS MAITRISENT :

- Les enquêtes et analyses sur les réseaux sociaux
- L'usage des réseaux sociaux et techniques de camouflages y liées
- Le contrôle et l'influence sur les groupes sociaux et membres affiliés
- Les techniques de manipulation sociales
- La publication a grande échelle d'informations et d'opinions
- L'exploitation des gisements d'informations sociales
- Le marketing de groupes et d'organisations

PROGRAMME ET DEROULEMENT DE LA FORMATION

- ***1er Partie : Les TIC, internet, les réseaux sociaux et le nouvel environnement social (ce qui a changé depuis)***
  - Nouvelles technologies de communication sociale ;
  - Carence de contrôle sur les réseaux sociaux et les conséquences sur la securite nationale
  - Le nouveau contexte social camerounais : adhésion aux reseaux sociaux, statistiques, intérêts des masses sociales et actions des groupes sociaux
- ***2ème Partie : usages et réalités des réseaux sociaux***
  - Etudes des réseaux sociaux comme : Facebook, Twiter, Wayn, linkedin, Hi5, myspace, youtube, wikkileaks, second life (jeux social en ligne);
  - Nouvelles relations sociales et politiques sur internet : Impact sur la vie réelle et conséquences sur la securite;
  - Camouflage social et recherche d'informations : cas pratiques
  - Organisation de la désinformation sociale : cas pratique
- ***3ème Partie : analyses sur la réalité du nouveau phénomène social***
  - Réseaux sociaux et surabondance de l'information et carence de confidentialité : le cas de wikkileaks
  - Réseaux sociaux : Rôles sur les récentes et actuelles crises politiques en Afrique ;
  - Quelles solutions pour l'avenir et comment maitriser les conséquences de l'usage abusif des réseaux sociaux

ITS – BP: 8570, Yaoundé-Cameroun; Web: http://www.groupits.cm;
Tel: (+237) 22070806, 22070848, 94031476, 79286931; Fax: +15817013252
Email: info@groupits.cm

SEMINAIRE DE FORMATION

GOUVERNANCE DES SI : NORMES ITIL et ValIT

Données de base

Etre un spécialiste du domaine des TIC ;
Un responsable d'entreprise et maitriser l'outil informatique, un responsable ou contrôleur dans une banque ou PME, un consultant en audit des SI ; un étudiant dans les TIC

Public cible

Toute personne déjà initiée aux services informatiques ou aux SI, à gérer l'ensemble des procédures ou à accompagner la fourniture des services informatiques, à définir une politique de gestion et de gouvernance du SI, à calculer le retour sur investissement ou à mettre sur pied un schéma directeur du S.I

Animateurs

1. **Christelle BIBEE (Cameroun)**

Master en Management des systèmes d'information ; consultante à ITS

2. **TCHATCHOU Christelle. (Cameroun)**

° Master en Management des systèmes d'information ; consultante à ITS

Méthodologie

Pédagogie active, réponses individualisées aux besoins des participants. Exposés théoriques, apports méthodologiques et nombreux travaux pratiques.
Chaque participant est invité à venir exposer ses besoins en sécurité et protection des SI.

Lieu

Kribi

Période

22, 23 et 24 MAI 2013

Durée

3 jours

Coût

900.000 Fcfa/ personne
Tarifs(HT) incluant les frais pédagogiques, les frais de documentation, les frais du matériel de formation et les frais de déjeuner pendant la formation. ***Un ordinateur portable offert à chaque participant.***

OBJECTIFS – AMENER LES PARTICIPANTS A :

- Cerner la notion de gouvernance des SI
- Maitriser les outils de mise en œuvre d'une gouvernance des SI
- Analyser la nécessité d'une bonne gouvernance du SI
- Etablir et améliorer le niveau de gouvernance de SI pour l'entreprise
- Mettre sur pied un schéma directeur du système d'information

RESULTATS ATTENDUS – LES PARTICIPANTS MAITRISENT :

- La notion de gouvernance du SI
- Les différents outils de mise en œuvre d'une gouvernance des systèmes d'information
- Les instruments de mesure de la maturité d'une gouvernance des SI
- Les méthodes d'amélioration de la gouvernance des SI

PROGRAMME ET DEROULEMENT DE LA FORMATION

- ***1er Jour : ITIL – Présentation générale***
  - Les concepts de fondamentaux;
  - Les différentes versions et organismes de certifications;
  - Les livres complémentaires.
- ***2ème Jour : les procédures de l'ITIL et ValIT***
  - Le soutien des services IT et ValIT
  - Le centre de services ou service desk; (gestion du changement, gestion des incidents, calcul du retour sur investissement des SI…)
  - L'importance de ces procédures. (gestion des configurations,..)
- ***3ème Jour : Planification et mise en œuvre de ITIL et ValIT***
  - La fourniture des services Informatiques; (Gestion financière, gestion de la capacité…)
  - Les éléments de couts et retour sur investissement en TIC
  - L'évaluation de la maturité.

Invité

1. **Prof. Jean-Robert KALA KAMDJOUG, (Cameroun)**

Professeur à l'Université Catholique d'Afrique Centrale, responsable du Master en Management des Systèmes d'information

Programme culturel

Débats chaque soir sur :
. 1. L'impact économique de la gestion des S.I. sur les entreprises
2. La mise en œuvre de ITIL et ValIT: enjeux et couts économiques
Visite des chutes de la LOBE

ITS – BP: 8570, Yaoundé-Cameroun; Web: http://www.groupits.cm;
Tel: (+237) 22070806, 22070848, 94031476, 79286931; Fax: +15817013252
Email: info@groupits.cm

SEMINAIRE DE FORMATION

SECURITE INFORMATIQUE ET PROTECTION DE L'INFORMATION

Données de base

Etre un spécialiste du domaine des TIC ;
Un responsable d'entreprise et maitriser l'outil informatique, un spécialiste du domaine de la sécurité (Police, Militaire etc.…), un responsable ou opérateur dans une banque, un Juriste ou associé ; un étudiant dans les TIC

Public cible

Toute personne déjà initiée ou non à la maitrise du risque métier dans un système d'information, à sécuriser ou à accompagner la sécurisation du SI, à définir la politique de sécurité du SI en entreprise, à rédiger les protocoles de sécurité du SI.

Animateurs

1. **Dr. BELL B.G.**

° PhD-sciences techniques en sécurité et protection des systèmes d'information ;
° Spécialiste en cryptologie (St. Petersburg) ;
° Expert en sécurité et protection des SI ;
° Enseignant-Chercheur (UCAC,ENSPY,UPAC)
° Directeur de ITS (www.groupits.cm)

2. **Dr. HELL Bonaventure**

- Docteur es sciences de l'information (Italy)
- Master en sécurité des TIC (Milan)
- Spécialiste en assurance qualité des TIC
- Directeur de ISQuality Sarl

Méthodologie

Pédagogie active, réponses individualisées aux besoins des participants. Exposés théoriques, apports méthodologiques et nombreux travaux pratiques.
Chaque participant est invité à venir exposer ses besoins en sécurité et protection des SI.

Lieu

Kribi

Période

24, 25, 26, 27 et 28 Juin 2013

Durée

5 jours

Coût

1.200.000 Fcfa/ personne

Tarifs(HT) incluant les frais pédagogiques, les frais de documentation, les frais du matériel de formation et les frais de déjeuner pendant la formation. ***Un ordinateur portable offert à chaque participant.***

OBJECTIFS – AMENER LES PARTICIPANTS A :

- Comprendre les mécanismes de sécurisation du système d'information
- Maitriser les principes et règles de gestion de la sécurité des SI
- Analyser les besoins en sécurité du système d'information
- Etablir et entretenir le niveau de sécurité acceptable pour l'entreprise
- Gérer le risque d'intrusion et de pénétration du SI

RESULTATS ATTENDUS – LES PARTICIPANTS MAITRISENT :

- L'élaboration d'une politique de sécurité du système d'information
- La mise en place des règles et protocoles de sécurité pour tous les usagers du SI
- L'usage d'Antivirus et la lutte contre les programmes malveillants
- La gestion de la sécurité du SI y compris la gestion des incidents et l'élaboration des plans de reprise d'activité après incidents
- La sécurité du réseau informatique

PROGRAMME ET DEROULEMENT DE LA FORMATION

- ***1er Jour : introduction à la sécurité informatique***
  - Objectifs de la sécurité informatique
  - La confidentialité et sécurité des données
  - Nécessité d'une approche globale de sécurité informatique
  - Mise en place d'une politique de sécurité informatique
- ***2ème Jour : virus et programmes malveillants***
  - Virus informatiques
  - Antivirus et solutions de sécurité informatique
  - Programmes espions : problèmes et solutions
  - Détection et traitement des virus et programmes espions dans les systèmes
- ***3ème Jour : sécurité sur Internet***
  - Risques liés à l'usage d'Internet
  - L'indispensable sécurité sur Internet
  - L'authentification
  - L'identification
- ***4ème Jour : cryptographie***
  - cryptographie dans la sécurité informatique
  - systèmes cryptographiques et applications
  - Les fonctions de la cryptographie
  - Systèmes de signature
- ***5ème Jour : Sécurité des technologies de réseaux et systèmes***
  - Les causes de l'insécurité des réseaux et systèmes informatiques
  - Les différents types de pirates informatiques
  - Le but et les procédés des cyber-agresseurs
  - Comment protéger son système informatique

ITS – BP: 8570, Yaoundé-Cameroun; Web: http://www.groupits.cm;
Tel: (+237) 22070806, 22070848, 94031476, 79286931; Fax: +15817013252
Email: info@groupits.cm

SEMINAIRE DE FORMATION

SECURITE INFORMATIQUE

Données de base

Etre un utilisateur des TIC ; Un responsable d'entreprise et maitriser l'outil informatique, responsable ou opérateur dans une banque, un Juriste ou associé ; Un gestionnaire d'actifs et valeurs liés aux TIC

Public cible

Toute personne déjà initiée ou non à la maitrise du risque métier dans un système d'information, à protéger les données et informations de valeurs, à mener des activités sans conséquences fâcheuses sur Internet et autres systèmes

Animateur

1. **Dr. BELL B.G. (Cameroun)**

° **PhD**-sciences techniques en sécurité et protection des systèmes d'information ;
° Spécialiste en cryptologie) ; expert en sécurité et protection des SI ;
° Chargé de cours associé à l'Université Catholique d'Afrique Centrale ;
° Enseignant-Chercheur à l'ENSPY
° Directeur de ITS (www.groupits.cm)

2. **Armel MEBANDE (Cameroun)** ;
Expert en sécurité des réseaux

Méthodologie

Pédagogie active, réponses individualisées aux besoins des participants. Exposés théoriques, apports méthodologiques et de nombreux travaux pratiques.

Chaque participant est invité à venir exposer ses besoins en sécurité et protection des SI.

Lieu

KRIBI

Période

22, 23 et 24 Juillet 2013

Durée

3 Jours

Coût

900.000 Fcfa/ personne

Tarifs incluant les frais pédagogiques, les frais de documentation et les frais de déjeuner pendant la formation. Un ordinateur portable offert à chaque participant.

OBJECTIFS – AMENER LES PARTICIPANTS A :

- Comprendre les menaces à la sécurité du système d'information
- Maitriser les principes et règles d'utilisation sans risque d'Internet et autres technologies
- Comprendre les besoins en sécurité du système d'information
- Etablir et entretenir le niveau de sécurité acceptable pour ses informations
- De gérer le risque d'exposition de ses informations
- Créer et garantir les conditions de sécurité de son identité sur internet
- Comprendre les risques liés à l'usage intensif des TIC

RESULTATS ATTENDUS – LES PARTICIPANTS MAITRISENT :

- La protection des données et informations personnelles
- Les risques liés à l'usage du téléphone, internet et autres réseaux
- Les mécanismes d'authentification, d'identification et de garantie d'intégrités des données
- Les techniques de protection contre les arnaques et autres attaques des systèmes d'information
- Les règles de bonnes pratiques informatiques
- Les mécanismes de protection de données confidentielles
- La gestion des risques TI

THEMES ET MODULES PEDAGOGIQUES

- *Introduction à la sécurité en milieu informatique*
- *management de la sécurité des systèmes d'information*
- *Bonnes pratiques en milieu informatique*
- *Protection des données*
- *Quelques outils de sécurité Informatique*

PROGRAMME ET DEROULEMENT DE LA FORMATION

1ee partie : *Introduction à la sécurité en milieu informatique : Risques, menaces, vulnérabilités et contre-mesures en milieu informatique*

2ème partie : *Environnement du management de la sécurité des systèmes d'information : méthodes et normes internationales de base*

3ème partie : *Bonnes pratiques en milieu informatique et conformité à la loi sur la cybersécurité et cybercriminalité au Cameroun*

4ème partie : *Protection des données confidentielles, authentification et assurance de l'intégrité des données et utilisateurs*

5ème partie : *Quelques logiciels de sécurité Informatique et astuces de sécurisation de son cyberespace : gestion des mots de passe et compte d'utilisateur ; gestion des codes de valeur ; gestion d'informations privées ; détection des menaces ; minimisation d'impacts des menaces ; respect des normes ; conseils divers…*

ITS – BP: 8570, Yaoundé-Cameroun; Web: http://www.groupits.cm;
Tel: (+237) 22070806, 22070848, 94031476, 79286931; Fax: +15817013252
Email: info@groupits.cm

SEMINAIRE DE FORMATION

AUDIT DES SYSTEMES D'INFORMATION:USAGE DU COBIT

Données de base

Etre un spécialiste du domaine des TIC ; Un responsable d'entreprise et maitriser l'outil informatique, un responsable ou contrôleur dans une banque ou PME, un consultant en audit des SI ; un étudiant dans les TIC

Public cible

Toute personne déjà initiée ou non à la gouvernance d'entreprise, amenée à assurer le contrôle et suivi des systèmes d'information d'une entreprise, à assurer la conformité du système d'information.

Animateurs

Christelle BIBEE (Cameroun).
Master en Management des systèmes d'information ; consultante à ITS

TCHATCHOU Christelle (Cameroun).
° Master en Management des systèmes d'information ; consultante à ITS

Méthodologie

Pédagogie active, réponses individualisées aux besoins des participants. Exposés théoriques, apports méthodologiques et nombreux travaux pratiques.
Chaque participant est invité à venir exposer ses besoins en gouvernance des SI.

Lieu

Kribi

Période

23, 24 et 25 Juillet 2013

Durée

3 jours

Coût

900.000 Fcfa/ personne

Tarifs(HT) incluant les frais pédagogiques, les frais de documentation, les frais du matériel de formation et les frais de déjeuner pendant la formation. ***Un ordinateur portable offert à chaque participant.***

OBJECTIFS – AMENER LES PARTICIPANTS A :

- Maitriser les différents domaines d'analyse du COBIT
- Identifier les différents processus portant organisation d'un SI
- Déterminer le niveau de maturité acceptable du SI
- Analyser les besoins et écarts par rapport au niveau acceptable
- Prendre des décisions convenables qui permettront d'améliorer de manière continue le SI

RESULTATS ATTENDUS – LES PARTICIPANTS MAITRISENT :

- Les domaines d'analyses selon le COBIT
- Les étapes d'un audit des SI
- L'usage de modèle de maturité des SI
- L'audit et le contrôle du systèmes d'information
- L'évolution de son SI

PROGRAMME ET DEROULEMENT DE LA FORMATION

- ***1er Jour : L'AUDIT DES SI***
  - Rappel sur l'audit du SI;
  - .Etapes de l'audit ;
  - Comparaison par rapport à un standard : COBIT
- ***2ème Jour : LE COBIT***
  - Présentation générale du COBIT
  - Les processus du COBIT (les domaines)
  - Les livres complémentaires
- ***3ème Jour : LE NIVEAU DE MATURITE DU SI***
  - Les niveaux de maturité du SI (mesure du niveau de maturité)
  - Les procédures de mesure (le CMMI)
  - L'amélioration continue du SI

Invités

1. **Dr BELL B.G ; PhD ; Directeur de ITS (Cameroun)**

2. **Prof. Jean Robert KALA KAMDJOUG (Cameroun)**

Professeur à l'Université Catholique d'Afrique Centrale, responsable du Master –Management des SI

Programme culturel

Débats chaque soir sur :

1. Mise en place du COBIT : couts économiques
2. Intérêts du COBIT

Visite des chutes de la LOBE

ITS – BP: 8570, Yaoundé-Cameroun; Web: http://www.groupits.cm;
Tel: (+237) 22070806, 22070848, 94031476, 79286931; Fax: +15817013252
Email: info@groupits.cm

SEMINAIRE DE FORMATION

SECURISATION DES SYSTEMES D'INFORMATION

Données de base

Etre un spécialiste du domaine des TIC ;
Un responsable d'entreprise et maitriser l'outil informatique, un spécialiste du domaine de la sécurité (Police, Militaire etc.…), un responsable ou opérateur dans une banque, un Juriste ou associé ; un étudiant dans les TIC

Public cible

Toute personne déjà initiée ou non à la maitrise du risque métier dans un système d'information, à sécuriser ou à accompagner la sécurisation du SI, à définir la politique de sécurité du SI en entreprise, à rédiger les protocoles de sécurité du SI.

Animateurs

1. **Dr. BELL B.G. (Cameroun)**

° PhD-sciences techniques en sécurité et protection des systèmes d'information;
° Spécialiste en cryptologie (St. Petersburg) ;
° Expert en sécurité et protection des SI ;
° Enseignant-Chercheur (UCAC,ENSPY,UPAC)
° Directeur de ITS (www.groupits.cm)

2. **Jerry KATHINGO (Kenya)**

o ISACA, CISM- Commetee Member.
o Expert en sécurité et protection des systèmes d'information.

Méthodologie

Pédagogie active, réponses individualisées aux besoins des participants. Exposés théoriques, apports méthodologiques et nombreux travaux pratiques.
Chaque participant est invité à venir exposer ses besoins en sécurité et protection des SI.

Lieu

Kribi

Période

20, 21 et 22 Août 2013

Durée

3 jours

Coût

900.000 Fcfa/ personne

Tarifs(HT) incluant les frais pédagogiques, les frais de documentation, les frais du matériel de formation et les frais de déjeuner pendant la formation. ***Un ordinateur portable est offert à chaque participant.***

OBJECTIFS – AMENER LES PARTICIPANTS A :

- Comprendre les mécanismes de sécurisation du système d'information
- Maitriser les principes et règles de gestion de la sécurité des SI
- Analyser les besoins en sécurité du système d'information
- Etablir et entretenir le niveau de sécurité acceptable pour l'entreprise
- Gérer le risque d'intrusion et de pénétration du SI

RESULTATS ATTENDUS – LES PARTICIPANTS MAITRISENT :

- Combat contre les virus et programmes espions
- Combat contre le piratage des systèmes d'information
- L'usage d'Antivirus et de la lutte contre les programmes malveillants
- L'audit et le contrôle de la sécurité des systèmes d'information
- La sécurité du réseau informatique

PROGRAMME ET DEROULEMENT DE LA FORMATION

- ***1er Jour : lutte contre les virus et programmes espions***
  - Destruction de virus et programmes espions;
  - Veille stratégique aux infections virales;
  - Veille stratégique à l'intrusion des programmes espions.
- ***2ème Jour : lutte contre le piratage des systèmes d'information***
  - Détection et prévention des intrusions illégales aux ordinateurs et systèmes d'information;
  - Usage des pare-feu et des systèmes de sécurité;
  - Cryptage de l'information.
- ***3ème Jour : audit et sécurité***
  - Gestion des risques sur les systèmes d'information;
  - Organisation de la sécurité dans les systèmes d'information;
  - Normes ISO 27001 et ISO 27002.

Invités

1. **Sergei VOROBEV (Fédération de Russie),**

Directeur de ICI PRO –
Gestion antivirale et sécurité contre programmes malveillants
Représentant de Kaspersky Labs et Dr WEB en zone CEMAC

2. **Prof. Hubert NGNODJOM (Cameroun),**

Professeur à l'Université Catholique d'Afrique Centrale, responsable du Master –Banques et Finances

Programme culturel

Débats chaque soir sur :
. 1. L'impact économique des risques informatiques sur les entreprises
2. Infections virales : enjeux et couts économiques
3. l'évolution de la malveillance informatique

Visite des chutes de la LOBE

ITS – BP: 8570, Yaoundé-Cameroun; Web: http://www.groupits.cm;
Tel: (+237) 22070806, 22070848, 94031476, 79286931; Fax: +15817013252
Email: info@groupits.cm

SEMINAIRE DE FORMATION

CYBERCRIMINALITE

Données de base

Etre un spécialiste du domaine de la sécurité (Police, Militaire etc.…), un Magistrat ou un investigateur, un spécialiste de l'informatique légale

Public cible

Toute personne déjà initiée ou non à traiter des dossiers de types cybercriminels, à sécuriser ou à accompagner la sécurisation du SI, à gérer les conflits liées aux systèmes d'information à travailler avec les systèmes d'information sensibles

Animateur

Dr. BELL B.G. (Cameroun)

° PhD-sciences techniques en méthodes et systèmes de protection de l'information, sécurité des informations et systèmes d'information ;
° Spécialiste en cryptologie (St. Petersburg) ;
° Expert en sécurité et protection des SI ;
° Enseignant-Chercheur (UCAC,ENSPY,UPAC)
° Directeur de ITS (www.groupits.cm)

Méthodologie

Pédagogie active, réponses individualisées aux besoins des participants.Exposés théoriques, apports méthodologiques et nombreux travaux pratiques.
Chaque participant est invité à venir exposer ses besoins en investigations numériques

Lieu

KRIBI

Période

26, 27 et 28 Août 2013

Durée

3 jours

Coût

900.000 Fcfa/ personne

Tarifs(HT) incluant les frais pédagogiques, les frais de documentation, les frais du matériel de formation et les frais de déjeuner pendant la formation. . Un ordinateur portable offert à chaque participant.

OBJECTIFS – AMENER LES PARTICIPANTS A :

- Comprendre l'environnement et les enjeux de la criminalité dans le cyberespace
- Maitriser les notions et concepts liés aux infractions dans les systèmes d'information
- Comprendre les mécanismes, procédés, et modes opératoires des cybercriminels
- Conduire et orienter les affaires cybercriminelles
- Maitriser les nouveaux risques d'infractions dans la société de l'information
- Maitre des moyens organisationnels et techniques de lutte contre la cybercriminalité

RESULTATS ATTENDUS – LES PARTICIPANTS MAITRISENT :

- Les technique et méthodes de lutte contre la criminalité informatique
- La gestion organisationnelle et technique des affaires liées à la cybercriminalité
- Les Notions et concepts liées à la cybercriminalité
- Les méthodes et systèmes de protection et sécurité du patrimoine numérique national
- La gestion des risques liés aux infractions dans la société de l'information
- L'analyse et la rédaction des rapports

PROGRAMME ET DEROULEMENT DE LA FORMATION

- ***1er Jour :***
  - Définitions et introduction à la cybercriminalité
  - Internet comme espace idéal dans l'évolution du cybercrime ;
  - Technologies facilitateurs de la cybercriminalité;
  - Loi sur la cybercriminalité au Cameroun : rapport avec les actions sur le terrain
- ***2ème Jour :***
  - Les motivations et intérêts pour la cybercriminalité : les outils de dissimulation d'activité et autres technologies
  - Cyber conflits et leurs enjeux stratégiques pour les Etats modernes
  - Frontières numériques et problématique de la coopération internationale dans la cybercriminalité
  - Moyens organisationnels et techniques de lutte contre le cybercrime
- ***3ème Jour :***
  - Gestion de la sécurité dans le cyberespace
  - Partage de responsabilités dans la sécurisation des biens numériques
  - Profil de cybercriminels dans le contexte Camerounais
  - Typologie du crime et délit informatique moderne

Invités

1. **Un juriste expert en cybercriminalité ;**
2. **Un commissaire de Police expert en investigations informatiques ;**
3. **Un responsable de l'entreprise DECISION-GROUP.**

Programme Culturel

Débats chaque soir sur :
1. Impact économique de la cybercriminalité au Cameroun ;
2. Les lois sur la cybercriminalité au Cameroun.

Visite des chutes de la LOBE

ITS – BP: 8570, Yaoundé-Cameroun; Web: http://www.groupits.cm;
Tel: (+237) 22070806, 22070848, 94031476, 79286931; Fax: +15817013252
Email: info@groupits.cm

SEMINAIRE DE FORMATION

PKI (Infrastructure de gestion des clés) : Rôle et usage dans la vérification et la confiance numérique

Données de base

Etre un spécialiste du domaine des TIC ;
Un responsable d'entreprise et maitriser l'outil informatique, un spécialiste du domaine de la sécurité (Police, Militaire etc.…), un responsable ou opérateur dans une banque, un Juriste ou associé ; un auditeur, contrôleur ou vérificateur dans les systèmes d'information, un étudiant dans les TIC

Public cible

Toute personne déjà initiée ou non à la maitrise du risque métier dans un système d'information, à sécuriser ou à accompagner la sécurisation du SI, à définir la politique de sécurité du SI en entreprise, à rédiger les protocoles de sécurité du SI.

Animateur

Dr. BELL B.G. (Cameroun)

° PhD-sciences techniques en sécurité et protection des systèmes d'information ;
° Spécialiste en cryptologie) ; expert en sécurité et protection des SI ;
° Enseignant-Chercheur (Ucac, Enspy, Upac, Enspt, Enam,Upec) ;
° Directeur de ITS (www.groupits.cm)

Méthodologie

Pédagogie active, réponses individualisées aux besoins des participants.
Exposé théorique, apports méthodologiques et nombreux travaux pratiques.
Chaque participant est invité à venir exposer ses besoins en sécurité et protection des SI.

Lieu

KRIBI

Période

16, 17, 18, 19 et 20 Septembre 2013

Durée

5 jours

Coût

1.200.000 Fcfa/personne

Tarifs(HT) incluant les frais pédagogiques, les frais de documentation, les frais du matériel de formation et les frais de déjeuner pendant la formation. Un ordinateur portable offert à chaque participant.

OBJECTIFS – AMENER LES PARTICIPANTS A :

- Comprendre et maitriser les mécanismes de cryptographie à clé publique
- Maitriser l'usage des protocoles de sécurité des systèmes d'information
- Implémenter et utiliser les systèmes de signature numérique
- Maitriser l'implémentation et l'utilisation de la certification numérique
- Maitriser la mise en place d'un système de vérification d'intégrité et de confidentialité des informations, processus, applications et entités numériques dans un système d'information

RESULTATS ATTENDUS – LES PARTICIPANTS MAITRISENT :

- L'élaboration d'une politique d'intégrité et de confidentialité dans un système d'information
- La mise en place des règles et protocoles de sécurité pour tous les usagers du SI
- L'utilisation de la signature et de la certification numériques dans la création des conditions de confiance numérique dans un système d'information
- Les applications de la PKI comme : La signature numérique ; La certification numérique ; La télé déclaration de la TVA ; Le notaire numérique ; la banque et systèmes de payements en ligne

PROGRAMME ET DEROULEMENT DE LA FORMATION

1er jour : Cryptographie dans la PKI

- Systèmes cryptographiques symétriques
- Systèmes cryptographiques asymétriques
- Fonctions de hachage

2e jour : PKI - Contrôle et la confiance dans les systèmes d'information

- La signature numérique et vérification de l'intégrité
- La certification numérique et vérification des identités
- Les déclarations et payements en ligne : Cas de la TVA, la banque en ligne et du notaire numérique

3e jour : Implémentation d'une PKI

- Mise en place d'une autorité de certification
- Création, modification, distribution et révocation des certificats
- Demande, édition, signature et conservation de certificats

4e jour : Gestion d'une PKI

- Autorité de certification racine
- Création, accréditation et gestion des autorités de certification et éditeurs de certificats
- Audit de fonctionnement d'une PKI

5e jour : Cas pratique

- Pratique de l'usage de la cryptographie asymétrique
- Pratique de l'usage de la signature et de la certification numérique
- Pratique d'usage et de la gestion d'une PKI

ITS – BP: 8570, Yaoundé-Cameroun; Web: http://www.groupits.cm;
Tel: (+237) 22070806, 22070848, 94031476, 79286931; Fax: +15817013252
Email: info@groupits.cm

SEMINAIRE DE FORMATION

INVESTIGATIONS NUMERIQUES

Données de base

Etre un spécialiste du domaine du contrôle, de la vérification, des investigations, de la sécurité et de l'informatique légale

Public cible

Toute personne déjà initiée ou non à mener une enquête dans un système d'information, à sécuriser ou à accompagner la sécurisation des preuves numériques, à chercher et trouver des preuves numériques d'infraction par ou dans un système d'information, à établir des protocoles de cyber enquêtes.

Animateurs

1. **Dr. BELL B.G. (Cameroun)**

° PhD-sciences techniques en sécurité et protection des systèmes d'information;
° Spécialiste en cryptologie (St. Petersburg) ;
° Expert en sécurité et protection des SI ;
° Enseignant Chercheur(UCAC,ENSPY,UPAC)
° Directeur de ITS (www.groupits.cm)

2. **Jerry KATHINGO (Kenya)**

o ISACA, CISM- Commetee Member.
o Expert en sécurité et protection des systèmes d'information.

Méthodologie

Pédagogie active, réponses individualisées aux besoins des participants. Exposés théoriques, apports méthodologiques et nombreux travaux pratiques.
Chaque participant est invité à venir exposer ses besoins en investigations numériques

Lieu

Kribi

Période

24, 25 et 26 Septembre 2013

Durée

3 jours

Coût

900.000 Fcfa/ personne

Tarifs(HT) incluant les frais pédagogiques, les frais de documentation, les frais du matériel de formation et les frais de déjeuner pendant la formation. ***Un ordinateur portable offert à chaque participant.***

OBJECTIFS – AMENER LES PARTICIPANTS A :

- Comprendre les méthodes et procédures d'investigations numériques
- Utiliser les ordinateurs et outils informatique dans la facilitation de l'établissement des preuves d'une infraction
- Maitriser la gestion de la preuve numérique
- Maitriser l'environnement des cyber enquêtes dans les systèmes informatiques (ordinateurs, téléphones portables, iPod, PDA, cartes a puce et autres)
- Analyser les porteurs d'information (clé USB, disques durs, Sim cartes) pour la détection des preuves d'infraction ou de délits
- L'usage des logiciels spéciaux de cyber enquêtes

RESULTATS ATTENDUS – LES PARTICIPANTS MAITRISENT :

- Les techniques d'investigations numériques
- La recherche des preuves numériques
- La gestion des preuves numériques
- La rédaction des rapports d'investigation numériques
- L'usage des logiciels spéciaux de cyber enquêtes
- L'environnement de la cybercriminalité (avant, pendant et après le crime)

Les portraits et méthodes d'intervention des cybercriminels

PROGRAMME ET DEROULEMENT DE LA FORMATION

PARTIE 1

- **1** : Définitions et introduction à l'investigation numérique
- **2** : **Fraude et crimes informatiques** au sein ou à l'encontre d'une organisation
- **3** : **Surveillance numérique**
- **4 : Preuves numériques** d'une infraction
- **5** : Récupération des **données effacées, cachées, cryptées**

PARTIE 2

- **1** : Recherche de **traces** visibles ou non d'une infraction numérique
- **2** : Méthodologie et démarche d'une investigation numérique
- **3** : Gestion de l'assistance technique dans les procédures **contentieuses ou précontentieuses** en investigation numérique
- **4** : Méthodes d'attaques de systèmes
- **5 : Rapports** d'investigation numérique

- Menaces, sources de menaces et degré de nuisance aux systèmes d'information

Invité

Un expert en investigations numériques du groupe DECISION-GROUP (Taiwan).

ITS – BP: 8570, Yaoundé-Cameroun; Web: http://www.groupits.cm;
Tel: (+237) 22070806, 22070848, 94031476, 79286931; Fax: +15817013252
Email: info@groupits.cm

SEMINAIRE DE FORMATION

AUDIT, VERIFICATION ET INVESTIGATIONS EN MILIEU INFORMATIQUE

Données de base

Etre un spécialiste du domaine du contrôle, de la vérification, des investigations, de la sécurité et de l'informatique légale

Public cible

Toute personne déjà initiée ou non à mener une enquête un contrôle ou une vérification dans un système d'information, à chercher et trouver des preuves numériques d'infractions par ou dans un système d'information, à établir des protocoles de cyber enquêtes, à rédiger les rapports d'audit, de contrôle et d'investigations en milieu informatique.

Animateurs

1. **Dr. BELL B.G. (Cameroun)**

° PhD-sciences techniques en sécurité et protection des systèmes d'information;
° Spécialiste en cryptologie (St. Petersburg) ;
° Expert en sécurité et protection des SI ;
° Enseignant-Chercheur(UCAC,ENSPY,UPAC)
° Directeur de ITS (www.groupits.cm)

2. **Prof. J.R. KALLA (Cameroun)**

Université Catholique d'Afrique Centrale
- Responsable du Master Management des systèmes d'information

Méthodologie

Pédagogie active, réponses individualisées aux besoins des participants. Exposés théoriques, apports méthodologiques et nombreux travaux pratiques.
Chaque participant est invité à venir exposer ses besoins en investigations

Lieu

KRIBI

Période

15, 16 et 17 Octobre 2013

Durée

3 jours

Coût

900.000 Fcfa/personne

Tarifs(HT) incluant les frais pédagogiques, les frais de documentation, les frais du matériel de formation et les frais de déjeuner pendant la formation. Un ordinateur portable offert à chaque participant.

OBJECTIFS – AMENER LES PARTICIPANTS A :

- Comprendre les méthodes et procédures d'investigations numériques
- Maitriser la gestion de la preuve numérique
- Maitriser l'environnement des cyber enquêtes dans les systèmes informatiques (ordinateurs, téléphones portables, iPod, PDA, cartes a puce et autres)
- L'usage des logiciels spéciaux de cyber enquêtes
- Connaitre des méthodes et moyens de vérification des systèmes d'information
- Maitriser les normes en matière d'audit et contrôle informatiques

Maitriser les méthodes d'audit informatique

RESULTATS ATTENDUS – LES PARTICIPANTS MAITRISENT :

- Les techniques d'investigations numériques, d'audit, de contrôle et de vérifications en milieu informatisé
- La recherche des preuves numériques
- La gestion des preuves numériques
- La rédaction des rapports d'investigation numériques et d'audit
- L'usage des logiciels spéciaux de cyber enquêtes
- L'environnement de la cybercriminalité (avant, pendant et après le crime)
- Les méthodes d'audit et de vérification informatiques

PROGRAMME ET DEROULEMENT DE LA FORMATION

PARTIE 1 : Audit et vérification informatiques

- **1** : Introduction à l'Audit et vérifications des systèmes et technologies de l'information
- **2** : Contrôles Généraux et d'applications des systèmes d'information
- **3** : Normes et standards en audit et vérifications informatiques (COBIT, ITIL et autres)
- **4 :** Logiciels d'audit et de vérification (IDEA Caseware)
- **5** : Rapports d'Audit

PARTIE 2 : Investigations Numériques

- 1 : Preuves numériques d'une infraction
- 2 : Méthodologie et démarche d'une investigation numérique
- 3 : Fraude et crimes informatiques au sein ou à l'encontre d'une organisation
- 4 : Surveillance numérique
- 5 : Rapports d'investigation numérique

ITS – BP: 8570, Yaoundé-Cameroun; Web: http://www.groupits.cm;
Tel: (+237) 22070806, 22070848, 94031476, 79286931; Fax: +15817013252
Email: info@groupits.cm

SEMINAIRE DE FORMATION

AUDIT ET CONTROLE DE LA SECURITE DES SYSTEMES D'INFORMATION

Données de base

Etre un spécialiste du domaine des TIC ;
Un responsable d'entreprise et maitriser l'outil informatique, un spécialiste du domaine de la sécurité (Police, Militaire etc.…), un responsable ou opérateur dans une banque, un Juriste ou associé ; un étudiant dans les TIC

Public cible

Toute personne déjà initiée ou non à la maitrise du risque métier dans un système d'information, à sécuriser ou à accompagner la sécurisation du SI, à définir la politique de sécurité du SI en entreprise, à rédiger les protocoles de sécurité du SI.

Animateur

Dr. BELL B.G. (Cameroun)

° PhD-sciences techniques en sécurité et protection des systèmes d'information;
° Spécialiste en cryptologie (St. Petersburg) ;
° Expert en sécurité et protection des SI ;
° Enseignant-Chercheur (UCAC,ENSPY, UPAC)
° Directeur de ITS (www.groupits.cm)

Méthodologie

Pédagogie active, réponses individualisées aux besoins des participants. Exposés théoriques, apports méthodologiques et nombreux travaux pratiques.
Chaque participant est invité à venir exposer ses besoins en sécurité et protection des SI.

Lieu

Kribi

Période

19, 20 et 21 Novembre 2013

Durée

3 jours

Coût

900.000 Fcfa/ personne

Tarifs(HT) incluant les frais pédagogiques, les frais de documentation, les frais du matériel de formation et les frais de déjeuner pendant la formation. ***Un ordinateur portable offert à chaque participant.***

OBJECTIFS – AMENER LES PARTICIPANTS A :

- Comprendre les mécanismes de lutte contre la cyber criminalité
- Maitriser l'audit de la sécurité des systèmes d'information
- Analyser et contrôler la sécurité du système d'information
- Etablir et entretenir le niveau de sécurité acceptable pour l'entreprise
- Mener des enquêtes sur les cyber crimes

RESULTATS ATTENDUS – LES PARTICIPANTS MAITRISENT :

- Les enquêtes et analyses sur les attaques des SI
- Le combat contre la cyber criminalité
- L'audit de la sécurité des systèmes d'information
- Les tests et le contrôle de la sécurité des systèmes d'information
- Le contrôle des menaces à la sécurité des SI

PROGRAMME ET DEROULEMENT DE LA FORMATION

- ***1er Jour : cybercriminalité (contrôle et enquêtes)***
  - Enquêtes sur ordinateurs et systèmes d'information ;
  - Analyse des ordinateurs, disques durs et systèmes d'information
  - Recherche et détection des traces de cyber crimes sur ordinateurs
- ***2ème Jour : contrôle des menaces***
  - Recherche et détection de programmes espions ;
  - Analyse et établissement de l'état de vulnérabilité des systèmes d'information ;
  - Analyse et détection des menaces à la sécurité des systèmes d'information
- ***3ème Jour : test de sécurité et évaluation des menaces***
  - Test et certification de conformité aux standards internationaux de sécurité informatique (ISO 27001 et autres);
  - Test de sécurité générale du système d'information ;
  - Menaces, sources de menaces et degré de nuisance aux systèmes d'information

Invité

1. **Sergei VOROBEV, (Fédération de Russie)**
   - Directeur de ICI PRO
   - Représentant de Kaspersky Labs et Dr WEB en zone CEMAC

Programme Culturel

Débats chaque soir sur :
1. Les enjeux stratégiques de la sécurité systèmes d'information
2. Le rôle de la norme internationale dans la sécurité des SI
3. problèmes de la coopération internationale dans la cybercriminalité

Partie de pêche en bateau sur l'atlantique

ITS – BP: 8570, Yaoundé-Cameroun; Web: http://www.groupits.cm;
Tel: (+237) 22070806, 22070848, 94031476, 79286931; Fax: +15817013252
Email: info@groupits.cm

SEMINAIRE DE FORMATION

" ERP / SAP " DANS LA GOUVERNANCE DES S.I.

Données de base

Etre un spécialiste du domaine des TIC ;
Un responsable d'entreprise et maîtriser l'ERP SAP,
Un directeur financier ou contrôleur de gestion (tout secteur d'activité),
Un consultant en audit des SI, en système d'information, en management ou en comptabilité,
Un étudiant dans les TIC et le management

Public cible

Toute personne déjà initiée ou non à l'utilisation de SAP, aux métiers dans un système d'information, à analyser les besoins en SI.

Animateurs

Aurélie CHIEGAING (France)
° Maitrise en Economie (UY2);
° Master en Management & Système d'information (UCAC);
° Msc in ComputerSc and IT Management (SUPINFO);
° Owner h@lo Consultancy Group: SAP Consulting & IT Management
www.group-halo.com

Méthodologie

Pédagogie active, réponses individualisées aux besoins des participants. Exposés théoriques, apports méthodologiques.

Chaque participant est invité à venir exposer ses besoins et projets SAP.

Lieu

Kribi

Période

19, 20 et 21 Novembre 2013

Durée

3 jours

Coût

900.000 Fcfa/ personne

Tarifs(HT) incluant les frais pédagogiques, les frais de documentation, les frais du matériel de formation et les frais de déjeuner pendant la formation. Un ordinateur portable offert à chaque participant.

OBJECTIFS – AMENER LES PARTICIPANTS A :

o Comprendre ce qu'est un ERP ainsi que ses avantages
o Maîtriser le progiciel: les modules fonctionnels & techniques
o Apprendre les différentes phase d'un projet SAP
o Comprendre le rôle de chaque d'acteur projet
o Comprendre l'importance de la conduite du changement dans un projet SAP

RESULTATS ATTENDUS – LES PARTICIPANTS MAITRISENT :

o L'importance d'un SI de type ERP (SAP)
o Les avantages et inconvénients d'un ERP (SAP)
o Les différentes phases d'un projet SAP et les modules fonctionnels & techniques
o L'importance de la conduite du changement dans un projet SAP et suivant la phase-projet
o Le rôle de chaque acteur-projet

PROGRAMME ET DEROULEMENT DE LA FORMATION

- ***1er Jour :*** ***Le SI de type ERP***
  - Définition, avantages et inconvénients;
  - Marché des ERP: SAP leader;
  - SAP et les secteurs d'activité.
- ***2 ème Jour: Projet SAP et acteurs-projet***
  - Phases/étapes du projet;
  - Acteurs-projet;
  - Modules fonctionnels & techniques.
- ***3ème Jour : Conduite du changement et gestion d'équipe***
  - Recherche de la cohésion d'équipe et communication;
  - Planification des ateliers de formation et d'information;
  - Communication.

Invités

1. Christelle BIBEE (Cameroun), Manager en systèmes d'information – Master en Management des systèmes d'information ;
2. Prof. KALA (Cameroun),
Professeur à l'Université Catholique d'Afrique Centrale, responsable du Master –Management des Systèmes d'informations

Programme culturel

Débats chaque soir sur :
. 1. Enjeux de la gouvernance du SI dans les entreprises camerounaises
2. apports de d'implémentation des ERP/SAP dans une entreprise
Visite des chutes de la LOBE

ITS – BP: 8570, Yaoundé-Cameroun; Web: http://www.groupits.cm;
Tel: (+237) 22070806, 22070848, 94031476, 79286931; Fax: +15817013252
Email: info@groupits.cm

CYBERSECURITE : ENJEUX ET NECESSITE POUR LA SOCIETE DE L'INFORMATION

Données de base

Etre un spécialiste du domaine de la sécurité (Police, Militaire etc.…), un élève de l'école de police ou de l'EMIA

Public cible

Toute personne déjà initiée ou non à la maitrise du risque métier dans un système d'information, à sécuriser ou à accompagner la sécurisation du SI, à définir la politique de sécurité des informations, à travailler avec les systèmes d'information sensibles

Animateurs

Dr. BELL B.G. (Cameroun)

° PhD-sciences techniques en méthodes et systèmes de protection de l'information, sécurité des informations ;
° Spécialiste en cryptologie (St. Petersburg) ;
° Expert en sécurité et protection des SI ;
° Enseignant-Chercheur (UCAC,ENSPY,UPAC)
° Directeur de ITS (www.groupits.cm)

Méthodologie

Pédagogie active, réponses individualisées aux besoins des participants. Exposés théoriques, apports méthodologiques et nombreux travaux pratiques.

Chaque participant est invité à venir exposer ses besoins en sécurité et protection des informations.

Lieu

Selon le client

Période

Selon le client

Durée

10 jours

Cout

Sur négociation

OBJECTIFS – AMENER LES PARTICIPANTS A :

- Comprendre les enjeux de la sécurité des systèmes d'information dans un monde au tout numérique
- Maitriser les notions et technique liées à la sécurité dans les systèmes d'information
- Comprendre les mécanismes et politiques de sécurité à l'ère du numérique
- Conduire et adapter le changement des systèmes de sécurité au nouveau type de société dite de l'information
- Maitriser les nouveaux risques dans la société de l'information
- Etablir les stratégies de sécurisation du cyberespace national

RESULTATS ATTENDUS – LES PARTICIPANTS MAITRISENT :

- Les technique et méthodes et de sécurité dans un environnement a dominance numérique
- Le combat contre les infractions et toute sorte de criminalité numériques
- L'usage de systèmes de sécurité des systemes d'information
- Les méthodes et systèmes de protection et sécurité du patrimoine numérique national
- La gestion des risques dans la société de l'information
- L'importance stratégique de la sécurité à l'ère du numérique

PROGRAMME ET DEROULEMENT DE LA FORMATION

- Définitions et introduction à la cyber sécurité
- l'usage d'internet comme arme de contrôle et de stabilisation des mouvements d'opinions et de la masse ;
- le contrôle et filtrage du trafic internet comme moyen de sécurisation du cyber espace;
- L'usage des systèmes d'information du renseignement – fichiers centraux de renseignement (judicaire, criminel, et autres)
- Le contrôle et le suivi des écoutes des canaux de transmission de l'information
- Cyber conflits et leurs enjeux stratégiques
- Frontières numériques et problématique de la coopération internationale dans la cyber sécurité
- Moyens organisationnels et techniques de la cyber sécurité
- Gestion de la sécurité dans le cyberespace
- Partage de responsabilités dans la sécurisation des biens numériques

ITS – BP: 8570, Yaoundé-Cameroun; Web: http://www.groupits.cm;
Tel: (+237) 22070806, 22070848, 94031476, 79286931; Fax: +15817013252
Email: info@groupits.cm

FORMATION A LA CARTE

RESEAUX SOCIAUX : ROLES ET USAGES DANS LA STRATEGIE DE SECURITE DES SOCIETES MODERNES

Données de base

Etre un spécialiste du domaine du contrôle, de la vérification, des investigations, de la sécurité et de l'informatique légale

Public cible

Toute personne déjà initiée ou non a la recherche de l'information, à créer ou accompagner la création d'opinions, à définir et orienter la politique et les objectifs de la masse sociale, a créer une motivation aux fin d'atteindre les objectifs de décision, a anticiper sur le comportement social pour mieux orienter les politiques de sécurité y liées

Animateurs

Dr. BELL B.G. (Cameroun)

° PhD-sciences techniques en sécurité et protection des systèmes d'information;
° Spécialiste en cryptologie (St. Petersburg) ;
° Expert en sécurité et protection des SI ;
° Enseignant-Chercheur (UCAC,ENSPY,UPAC)
° Directeur de ITS (www.groupits.cm)

Méthodologie

Pédagogie active, réponses individualisées aux besoins des participants. Exposés théoriques, apports méthodologiques et nombreux travaux pratiques.
Chaque participant est invité à venir exposer ses besoins en usage des réseaux sociaux

Lieu

Selon le client

Période

Au choix du client

Durée

10 jours

Coût

Sur négociation / personne

OBJECTIFS – AMENER LES PARTICIPANTS A :

- Comprendre les mécanismes de sécurité a l'ère du numérique
- Comprendre l'usage des réseaux sociaux comme arme informationnelle
- Comprendre la désinformation sociale et guerre informationnelles
- Maitriser le phénomène de camouflage social
- Utiliser les réseaux sociaux comme gites informationnelles

RESULTATS ATTENDUS – LES PARTICIPANTS MAITRISENT :

- Les enquêtes et analyses sur les réseaux sociaux
- L'usage des réseaux sociaux et techniques de camouflages y liées
- Le contrôle et l'influence sur les groupes sociaux et membres affiliés
- Les techniques de manipulation sociales
- La publication a grande échelle d'informations et d'opinions
- L'exploitation des gisements d'informations sociales
- Le marketing de groupes et d'organisations

PROGRAMME ET DEROULEMENT DE LA FORMATION

- ***1er Partie : Les TIC, internet, les réseaux sociaux et le nouvel environnement social (ce qui a changé depuis)***
  - Nouvelles technologies de communication sociale ;
  - Carence de contrôle sur les réseaux sociaux et les conséquences sur la securite nationale
  - Le nouveau contexte social camerounais : adhésion aux reseaux sociaux, statistiques, intérêts des masses sociales et actions des groupes sociaux
- ***2ème Partie : usages et réalités des réseaux sociaux***
  - Etudes des réseaux sociaux comme : Facebook, Twiter, Wayn, linkedin, Hi5, myspace, youtube, wikkileaks, second life (jeux social en ligne);
  - Nouvelles relations sociales et politiques sur internet : Impact sur la vie réelle et conséquences sur la securite;
  - Camouflage social et recherche d'informations : cas pratiques
  - Organisation de la désinformation sociale : cas pratique
- ***3ème Partie : analyses sur la réalité du nouveau phénomène social***
  - Réseaux sociaux et surabondance de l'information et carence de confidentialité : le cas de wikkileaks
  - Réseaux sociaux : Rôles sur les récentes et actuelles crises politiques en Afrique ;
  - Quelles solutions pour l'avenir et comment maitriser les conséquences de l'usage abusif des réseaux sociaux

ITS – BP: 8570, Yaoundé-Cameroun; Web: http://www.groupits.cm;
Tel: (+237) 22070806, 22070848, 94031476, 79286931; Fax: +15817013252
Email: info@groupits.cm

FORMATION A LA CARTE

AUDIT ET VERIFICATION INFORMATIQUE

Données de base

Etre un spécialiste du domaine des TIC ;
Un responsable d'audit et contrôle ; un cadre des services de contrôles et d'enquêtes

Public cible

Toute personne déjà initiée ou non à la maitrise du risque métier dans un système d'information, à auditer ou accompagner l'audit et le contrôle dans un système d'information ou à l'aide d'un système d'information

1. Dr. BELL B.G. (Cameroun)

° PhD-sciences techniques en sécurité et protection des systèmes d'information;
° Spécialiste en cryptologie (St. Petersburg) ;
° Expert en sécurité et protection des SI ;
° Enseignant-Chercheur(UCAC,ENSPY,UPAC)
° Directeur de ITS (www.groupits.cm)

Méthodologie

Pédagogie active, réponses individualisées aux besoins des participants. Exposés théoriques, apports méthodologiques et nombreux travaux pratiques.
Chaque participant est invité à venir exposer ses besoins en Audit et contrôle des systèmes d'information.

Lieu

Yaoundé, Douala, Kribi ou Limbe

Période

Selon le client

Durée

2 semaines

Coût

Sur négociation

Tarifs incluant les frais pédagogiques et les frais de documentation

OBJECTIFS – AMENER LES PARTICIPANTS A :

- Connaitre des méthodes et moyens de vérification des systèmes d'information
- Maitriser les normes en matière d'audit et contrôle informatiques
- Maitriser les méthodes d'audit informatique
- Evaluer les méthodes d'audit et de contrôle informatiques
- Maitriser l'usage de logiciels d'audit et de vérification informatique
- S'adapter à l'environnement informatique pour la vérification
- Etablir des relations entre vérifications informatisée et manuelle

RESULTATS ATTENDUS – LES PARTICIPANTS MAITRISENT :

- Les notions et concepts liés à l'audit et à la vérification informatique
- Les techniques d'audit et de vérifications informatiques
- L'environnement pratique d'audit et de vérification informatique
- Les logiciels d'audit et de vérification informatique
- La rédaction des rapports d'audit informatique

PROGRAMME ET DEROULEMENT DE LA FORMATION

- **SEMAINE 1** :
  1er Jour : Technologies de l'information et systèmes d'information
- ***2ème Jour :*** Introduction à l'Audit et vérification des systèmes et technologies de l'information

  3ème Jour : Analyse et gestion des risques

  4ème Jour **:** Contrôles généraux

  5ème Jour : Contrôles d'applications
- **SEMAINE 2 :**
  1er Jour : Logiciels d'audit et de vérification (IDEA Caseware)

  2ème Jour : Norme et standard en audit et vérifications(COBIT)

  3ème Jour : La Sécurité et la vérification des Systèmes de Gestion des bases de données SGBD

  4ème Jour : L'échantillonnage statistique en audit et vérification

  5ème Jour **:** Rapports d'Audit

ITS – BP: 8570, Yaoundé-Cameroun; Web: http://www.groupits.cm;
Tel: (+237) 22070806, 22070848, 94031476, 79286931; Fax: +15817013252
Email: info@groupits.cm

FORMATION A LA CARTE

AUDIT, VERIFICATION ET INVESTIGATIONS EN MILIEU INFORMATIQUE

Données de base

Etre un spécialiste du domaine du contrôle, de la vérification, des investigations, de la sécurité et de l'informatique légale

Public cible

Toute personne déjà initiée ou non à mener une enquête un contrôle ou une vérification dans un système d'information, à chercher et trouver des preuves numériques d'infractions par ou dans un système d'information, à établir des protocoles de cyber enquêtes, à rédiger les rapports d'audit, de contrôle et d'investigations en milieu informatique.

Animateur

1. Dr. BELL B.G. (Cameroun)

° PhD-sciences techniques en sécurité et protection des systèmes d'information;
° Spécialiste en cryptologie (St. Petersburg) ;
° Expert en sécurité et protection des SI ;
° Enseignant-Chercheur(UCAC,ENSPY,UPAC)
° Directeur de ITS (www.groupits.cm)

2. Prof. J.R. KALLA (Cameroun)
Université Catholique d'Afrique Centrale

- Responsable du Master Management des systèmes d'information

Méthodologie

Pédagogie active, réponses individualisées aux besoins des participants. Exposés théoriques, apports méthodologiques et nombreux travaux pratiques.
Chaque participant est invité à venir exposer ses besoins en investigations numériques

Lieu

Yaoundé, Douala, Kribi ou Limbe

Période

Selon le client

Durée

2 semaines

Coût

Sur négociation

OBJECTIFS – AMENER LES PARTICIPANTS A :

- Comprendre les méthodes et procédures d'investigations numériques
- Maitriser la gestion de la preuve numérique
- Maitriser l'environnement des cyber enquêtes dans les systèmes informatiques (ordinateurs, téléphones portables, iPod, PDA, cartes a puce et autres)
- L'usage des logiciels spéciaux de cyber enquêtes
- Connaitre des méthodes et moyens de vérification des systèmes d'information
- Maitriser les normes en matière d'audit et contrôle informatiques
- Maitriser les méthodes d'audit informatique

RESULTATS ATTENDUS – LES PARTICIPANTS MAITRISENT :

- Les techniques d'investigations numériques, d'audit, de contrôle et de vérifications en milieu informatisé
- La recherche des preuves numériques
- La gestion des preuves numériques
- La rédaction des rapports d'investigation numériques et d'audit
- L'usage des logiciels spéciaux de cyber enquêtes
- L'environnement de la cybercriminalité (avant, pendant et après le crime)
- Les méthodes d'audit et de vérification informatiques

PROGRAMME ET DEROULEMENT DE LA FORMATION

SEMAINE 1 : Audit et vérification informatiques

- **Jour 1** : Introduction à l'Audit et vérifications des systèmes et technologies de l'information
- **Jour 2** : Contrôles Généraux et d'applications des systèmes d'information
- **Jour 3** : Normes et standards en audit et vérifications informatiques (COBIT, ITIL et autres)
- **Jour 4 :** Logiciels d'audit et de vérification (IDEA Caseware)
- **Jour 5** : Rapports d'Audit

SEMAINE 2 : Investigations Numériques

- **Jour 1** : **Preuves numériques** d'une infraction
- **Jour 2** : Méthodologie et démarche d'une investigation numérique
- **Jour 3** : **Fraude et crimes informatiques** au sein ou à l'encontre d'une organisation
- **Jour 4** : **Surveillance numérique**
- **Jour 5 : Rapport** d'investigation numérique

ITS – BP: 8570, Yaoundé-Cameroun; Web: http://www.groupits.cm;
Tel: (+237) 22070806, 22070848, 94031476, 79286931; Fax: +15817013252
Email: info@groupits.cm

INVESTIGATIONS NUMERIQUES

Données de base

Etre un spécialiste du domaine du contrôle, de la vérification, des investigations, de la sécurité et de l'informatique légale

Public cible

Toute personne déjà initiée ou non à mener une enquête dans un système d'information, à sécuriser ou à accompagner la sécurisation des preuves numériques, à chercher et trouver des preuves numériques d'infraction par ou dans un système d'information, à établir des protocoles de cyber enquêtes.

Animateurs

1. **Dr. BELL B.G. (Cameroun)**

° PhD-sciences techniques en sécurité et protection des systèmes d'information;
° Spécialiste en cryptologie (St. Petersburg) ;
° Expert en sécurité et protection des SI ;
° Enseignant-Chercheur(UCAC,ENSPY,UPAC)
° Directeur de ITS (www.groupits.cm)

2. **Un expert en investigations numériques de DECISION-GROUP**

Méthodologie

Pédagogie active, réponses individualisées aux besoins des participants. Exposés théoriques, apports méthodologiques et nombreux travaux pratiques.
Chaque participant est invité à venir exposer ses besoins en investigations numériques

Lieu

Yaoundé, Douala, Kribi ou Limbe

Période

Selon le client

Durée

2 semaines

Coût

Sur négociation

Tarifs incluant les frais pédagogiques et les frais de documentation

OBJECTIFS – AMENER LES PARTICIPANTS A :

- Comprendre les méthodes et procédures d'investigations numériques
- Utiliser les ordinateurs et outils informatique dans la facilitation de l'établissement des preuves d'une infraction
- Maitriser la gestion de la preuve numérique
- Maitriser l'environnement des cyber enquêtes dans les systèmes informatiques (ordinateurs, téléphones portables, iPod, PDA, cartes a puce et autres)
- Analyser les porteurs d'information (clé USB, disques durs, Sim cartes) pour la détection des preuves d'infraction ou de délits
- L'usage des logiciels spéciaux de cyber enquêtes

RESULTATS ATTENDUS – LES PARTICIPANTS MAITRISENT :

- Les techniques d'investigations numériques
- La recherche des preuves numériques
- La gestion des preuves numériques
- La rédaction des rapports d'investigation numériques
- L'usage des logiciels spéciaux de cyber enquêtes
- L'environnement de la cybercriminalité (avant, pendant et après le crime)
- Les portraits et méthodes d'intervention des cybercriminels

PROGRAMME ET DEROULEMENT DE LA FORMATION

SEMAINE 1

- **Jour 1** : Définitions et introduction à l'investigation numérique
- **Jour 2** : **Fraude et crimes informatiques** au sein ou à l'encontre d'une organisation
- **Jour 3** : **Surveillance numérique**
- **Jour 4 : Preuves numériques** d'une infraction
- **Jour 5** : Récupération des **données effacées, cachées, cryptées**

SEMAINE 2

- **Jour 1** : Recherche de **traces** visibles ou non d'une infraction numérique
- **Jour 2** : Méthodologie et démarche d'une investigation numérique
- **Jour 3** : Gestion de l'assistance technique dans les procédures **contentieuses ou précontentieuses** en investigation numérique
- **Jour 4** : Méthodes d'attaques de systèmes
- **Jour 5 : Rapport** d'investigation numérique

ITS – BP: 8570, Yaoundé-Cameroun; Web: http://www.groupits.cm;
Tel: (+237) 22070806, 22070848, 94031476, 79286931; Fax: +15817013252
Email: info@groupits.cm

FORMATION A LA CARTE

SECURISATION DU SYSTEME D'INFORMATION D'UNE ENTREPRISE

Données de base

Etre un spécialiste du domaine des TIC ;
Un responsable d'entreprise et maitriser l'outil informatique, un spécialiste du domaine de la sécurité (Police, Militaire etc.…), un responsable ou opérateur dans une banque, un Juriste ou associé ; un étudiant dans les TIC

Public cible

Toute personne déjà initiée ou non à la maitrise du risque métier dans un système d'information, à sécuriser ou à accompagner la sécurisation du SI, à définir la politique de sécurité du SI en entreprise, à rédiger les protocoles de sécurité du SI.

Animateurs

2. Dr. BELL B.G. (Cameroun)

° PhD-sciences techniques en sécurité et protection des systèmes d'information;
° Spécialiste en cryptologie (St. Petersburg) ;
° Expert en sécurité et protection des SI ;
° Enseignant-Chercheur (UCAC,ENSPY,UPAC)
° Directeur de ITS (www.groupits.cm)

2. Jerry KATHINGO (Kenya)

o ISACA, CISM- Commetee Member.
o Expert en sécurité et protection des systèmes

Méthodologie

Pédagogie active, réponses individualisées aux besoins des participants. Exposé théorique, apports méthodologiques et nombreux travaux pratiques.

Chaque participant est invité à venir exposer ses besoins en sécurité et protection des SI.

Lieu

Yaoundé, Douala, Kribi ou Limbe

Période

Selon le client

Durée

2 semaines

Coût

Sur négociation

Tarifs incluant les frais pédagogiques, et les frais de documentation

OBJECTIFS – AMENER LES PARTICIPANTS A :

- Comprendre les mécanismes de sécurisation du système d'information
- Maitriser les principes et règles de gestion de la sécurité des SI
- Analyser les besoins en sécurité du système d'information
- Etablir et entretenir le niveau de sécurité acceptable pour l'entreprise
- Gérer le risque d'intrusion et de pénétration du SI

RESULTATS ATTENDUS – LES PARTICIPANTS MAITRISENT :

- L'élaboration d'une politique de sécurité du système d'information
- La mise en place des règles et protocoles de sécurité pour tous les usagers du SI
- L'audit de la sécurité du système d'information
- La gestion de la sécurité du SI y compris la gestion des incidents et l'élaboration des plans de reprise d'activité après incidents

THEMES ET MODULES PEDAGOGIQUES

1. Audit et control de la sécurité des systèmes d'information
2. Analyse du risque informationnel
3. Maintenance du système de sécurité et protection informatique
4. Management de la sécurité des systèmes d'information
5. PKI et Cryptologie
6. Implémentation des systèmes de sécurité et protection informatique
7. Intégration de solutions de sécurité des systèmes d'information
8. Anti-virus et programmes malveillants
9. Sécurité des technologies de réseaux informatiques
10. Plan de reprise d'activités

DEROULEMENT DE LA FORMATION

- **SEMAINE 1** :

  1er Jour : Audit et contrôle de la sécurité des systèmes d'information
- ***2ème Jour :*** Analyse du risque informationnel dans un système d'information
  3ème Jour : Maintenance du système de sécurité et protection informatique
- ***4ème Jour*** **:** Management de la sécurité des systèmes d'information.
  5ème Jour : PKI et cryptologie

- **SEMAINE 2 :**

  1er Jour : Implémentation des systèmes de sécurité et protection informatique
  2ème Jour : Intégration des solutions de sécurité des systèmes d'information
  3ème Jour : Anti-virus et programmes malveillants
  4ème Jour : Sécurité des technologies de réseaux informatiques
  5ème Jour **:** Cyber guerres et cyber conflits : enjeux

ITS – BP: 8570, Yaoundé-Cameroun; Web: http://www.groupits.cm;
Tel: (+237) 22070806, 22070848, 94031476, 79286931; Fax: +15817013252
Email: info@groupits.cm

FORMATION A LA CARTE

SECURITE INFORMATIQUE

Données de base

Etre un utilisateur des TIC ; Un responsable d'entreprise et maitriser l'outil informatique, responsable ou opérateur dans une banque, un Juriste ou associé ; Un gestionnaire d'actifs et valeurs liés aux TIC

Public cible

Toute personne déjà initiée ou non à la maitrise du risque métier dans un système d'information, à protéger les données et informations de valeurs, à mener des activités sans conséquences fâcheuses sur Internet et autres systèmes

Animateurs

1. **Dr. BELL B.G. (Cameroun)**

° **PhD**-sciences techniques en sécurité et protection des systèmes d'information, ; ° Spécialiste en cryptologie) ; expert en sécurité et protection des SI ;
° Chargé de cours associé à l'Université Catholique d'Afrique Centrale ;
° Enseignant-Chercheur à l'ENSPY
° Directeur de ITS (www.groupits.cm)

2. **Armel MEBANDE (Cameroun) ;**

Expert en sécurité des réseaux

Méthodologie

Pédagogie active, réponses individualisées aux besoins des participants. Exposés théoriques, apports méthodologiques et de nombreux travaux pratiques.

Chaque participant est invité à venir exposer ses besoins en sécurité et protection des SI.

Lieu

Yaoundé, Douala, Kribi ou Limbe

Période

Selon le client

Durée

2 semaines

Coût

Sur négociation

Tarifs incluant les frais pédagogiques, les frais de documentation

OBJECTIFS – AMENER LES PARTICIPANTS A :

- Comprendre les menaces à la sécurité du système d'information
- Maitriser les principes et règles d'utilisation sans risque d'Internet et autres technologies
- Comprendre les besoins en sécurité du système d'information
- Etablir et entretenir le niveau de sécurité acceptable pour ses informations
- De gérer le risque d'exposition de ses informations
- Créer et garantir les conditions de sécurité de son identité sur internet
- Comprendre les risques liés à l'usage intensif des TIC

RESULTATS ATTENDUS – LES PARTICIPANTS MAITRISENT :

- La protection des données et informations personnelles
- Les risques liés à l'usage du téléphone, internet et autres réseaux
- Les mécanismes d'authentification, d'identification et de garantie d'intégrités des données
- Les techniques de protection contre les arnaques et autres attaques des systèmes d'information
- Les règles de bonnes pratiques informatiques
- Les mécanismes de protection de données confidentielles
- La gestion des risques TI

THEMES ET MODULES PEDAGOGIQUES

- *Introduction à la sécurité en milieu informatique*
- *management de la sécurité des systèmes d'information*
- *Bonnes pratiques en milieu informatique*
- *Protection des données*
- *Quelques outils de sécurité Informatique*

PROGRAMME ET DEROULEMENT DE LA FORMATION

1ee partie : *Introduction à la sécurité en milieu informatique : Risques, menaces, vulnérabilités et contre-mesures en milieu informatique*

2ème partie : *Environnement du management de la sécurité des systèmes d'information : méthodes et normes internationales de base*

3ème partie : *Bonnes pratiques en milieu informatique et conformité à la loi sur la cybersécurité et cybercriminalité au Cameroun*

4ème partie : *Protection des données confidentielles, authentification et assurance de l'intégrité des données et utilisateurs*

5ème partie : *Quelques logiciels de sécurité Informatique et astuces de sécurisation de son cyberespace : gestion des mots de passe et compte d'utilisateur ; gestion des codes de valeur ; gestion d'informations privées ; détection des menaces ; minimisation d'impacts des menaces ; respect des normes ; conseils divers…*

ITS – BP: 8570, Yaoundé-Cameroun; Web: http://www.groupits.cm;
Tel: (+237) 22070806, 22070848, 94031476, 79286931; Fax: +15817013252
Email: info@groupits.cm

FICHE D'INSCRIPTION AUX SEMINAIRES

Nom de l'organisation: ……

Adresse :……..Tel : ……Email :……

Nombre de participants : …..... période :……..……

Thème du séminaire :……...

Visa du responsable (nom, signature et cachet):……..…..……

Nom et prénom du participant	Remarques et commentaires

Modes de payement

Les payements se font au nom de « CF-ITS » par bons d'engagement (pour les ministères et organes de l'Etat), chèques ou versements au compte bancaire (BICEC) suivant: 10001-06861-52557561001-48

NB : vous pouvez télécharger cette fiche dans http://www.groupits.cm

ILS NOUS FONT CONFIANCE !!!

MINEPAT/PNDP

CRTV

COBAC

PRESIDENCE DU CAMEROUN

AN

CENADI

TRACTAFRIC

Tractafric equipment CAT

Cameroon

SHO-TRACTAFRIC

CNIC

CHANTIER NAVAL

CAMEROUN-UNION EUROPEENE

CAONFED

CAONFED

CCA MICROFINANCE

CCA

sni

Société Nationale d'Investissement du Cameroun

SNI

CAMPOST

REPUBLIQUE DU CAMEROUN

Contrôle Superieur de l'ETAT

CONSUPE

REPUBLIQUE DU CAMEROUN

Ministere de la defense

MINDEF

REPUBLIQUE DU CAMEROUN

Ministere de la culture

MINCULT

REPUBLIQUE DU CAMEROUN

Ministere de la communication

MINCOM

REPUBLIQUE DU CAMEROUN

Ministere des travaux publics

MINTP

REPUBLIQUE DU CAMEROUN

Ministere de la justice

MINJUSTICE

REPUBLIQUE DU CAMEROUN

Ministere du commerce

MINCOMMERCE

REPUBLIQUE DU CAMEROUN

Ministere des forets et de la faune

MINFOF

ALPHA ASSURANCES S.A.

Une autre manière d'être assuré

ALPHA ASSURANCES

BEAC

NPS

CNPS

banque atlantique

BANQUE ATLANTIQUE

CONSEIL NATIONAL DES CHARGEURS DU CAMEROUN

CAMEROON NATIONAL SHIPPERS' COUNCIL

CNCC

CFC

CREDIT FONCIER DU CAMEROUN

GUCE

GUCE

UNITE PROGRES TRAVAIL

PRESIDENCE DU TCHAD