|  |  |  |
| --- | --- | --- |
| **REPUBLIQUE DU CAMEROUN**  **Paix - Travail - Patrie**  **----------------------** | C:\Users\DELL\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Logo MINDCAF.PNG | **REPUBLIC OF CAMEROON**  **Peace - Work - Fatherland**  **------------------** |
| **MINISTERE DES POSTES ET TELECOMMUNICATIONS**  **------------------** | **MINISTRY OF POSTS AND TELECOMMUNICATION**  **------------------** |

**RENFORCEMENT DES CAPACITES DU PERSONNEL DU MINPOSTEL EN MATIERE DE CYBER SECURITE.**

**MARCHE N° 0000038/M/MPT/SG/DAG/2021 DU 15/10/2021**

**PASSE APRES APPEL D’OFFRES NATIONAL RESTREINT N°00000026/AONR/MPT/CIPM/2021 DU 17 AOUT 2021 LANCE EN PROCEDURE D’URGENCE POUR LE RECRUTEMENT D’UN CABINET OU BUREAU D’ETUDES EN VUE DU RENFORCEMENT DES CAPACITES DU PERSONNEL DU MINPOSTEL EN MATIERE DE CYBER SECURITE.**

**RAPPORT DE LA FORMATION SUR ISO 27001 LEAD AUDITOR**

**Novembre 2021**





**RAPPORT DE LA FORMATION SUR ISO 27001 LEAD AUDITOR**





LE PRESENT DOCUMENT EST LE RAPPORT DE LA FORMATION SUR LE MODULE ISO 27001 LEAD AUDITOR DANS LE CADRE DU MARCHE N° 00000038/M/MPT/SG/DAG/2021 DU 15/10/2021

PASSE APRES APPEL D’OFFRES NATIONAL RESTREINT N°00000026/AONR/MPT/CIPM/2021 DU 17 AOUT 2021 LANCE EN PROCEDURE D’URGENCE POUR LE RECRUTEMENT D’UN CABINET OU BUREAU D’ETUDES EN VUE DU RENFORCEMENT DES CAPACITES DU PERSONNEL DU MINPOSTEL EN MATIERE DE CYBER SECURITE.

Tous droits réservés. Aucune partie de ce document ne peut être reproduite, mise en mémoire dans un système de recherche bibliographique ni transmis sous quelque forme ou par quelques procédés que ce soit électronique, mécanique, par photocopie ou autres sans autorisation préalable. Adresser une demande motivée, en indiquant les passages ou illustrations en cause au MINPOSTEL maitre d’ouvrage de cette étude susmentionnée.

**SOMMAIRE**

[**1.** **AVANT-PROPOS** 6](#_Toc90062988)

[**2.** **Introduction et contexte** 7](#_Toc90062989)

[**3.** **Objectifs de la formation** 9](#_Toc90062990)

[3.1. Objectif général 9](#_Toc90062991)

[3.2. Objectifs spécifiques 9](#_Toc90062992)

[**4.** **Méthodologie choisie** 10](#_Toc90062993)

[**5.** **Déroulement de la formation** 11](#_Toc90062994)

[**6.** **Domaines abordés** 13](#_Toc90062995)

[**7.** **Conclusion** 15](#_Toc90062996)

[ANNEXES 16](#_Toc90062997)

[A1/ ATTESTATIONS DE PARTICIPATION 17](#_Toc90062998)

[A2/ LISTES DE PRESENCE 20](#_Toc90062999)

[A3/ PHOTOS DE FAMILLE 26](#_Toc90063000)

# **AVANT-PROPOS**

Le présent document est confidentiel et sa confidentialité consiste à :

* La non divulgation des informations de configurations et paramétrages auprès de tierce partie ;
* La non reproduction des informations considérées confidentielles, sauf accord du Ministère des Postes et Télécommunications ;
* Les savoir-faire y contenus ne doivent profiter qu’au Ministère des Postes et Télécommunications ;
* Considérer toutes les informations déclarées Confidentielles.

# **Introduction et contexte**

La sécurité électronique est un enjeu majeur pour toutes les strates de la société et toutes les catégories de la population tant au niveau national qu’international. En quelques décennies l’espace numérique ou cyberespace est devenu un lieu de convoitise et d’affrontements pour les grandes puissances qui ont bien mesuré son caractère stratégique.

Le cyberespace se distingue dans les réalités traditionnelles par l’intangibilité des échanges qui s’y déroulent et l’interactivité entre les différents utilisateurs du réseau. Il a par ailleurs un caractère supranational qui, renforcé par l’autonomie du réseau internet n’y facilite pas l’application des principes juridiques traditionnels. De ce fait, de nombreux risques y naissent et rendent vulnérables toutes les entités qui le côtoient.

Conscient de ce qui précède, l’État du Cameroun a créé au sein de son Ministère des Poste et Télécommunications une Direction de la Sécurité des Réseaux et des Système d’Information. La mission assignée à cette Direction est de résoudre les difficultés liées à la sécurité informatique et cybersécurité sur l’ensemble du territoire national.

Seulement, toutes les analyses démontrent que la Direction de la Sécurité des Réseaux et des Système d’Information n’est pas suffisamment outillées en matière de compétences pour pouvoir répondre efficacement à cette mission. C’est dans le but d’apporter un début de solution à ces problèmes que le marché « N° 0000038/M/MPT/SG/DAG/2021 DU 15/10/2021 passé après appel d’offres national restreint N°00000026/AONR/MPT/CIPM/2021 du 17 aout 2021 lance en procédure d’urgence pour le recrutement d’un cabinet ou bureau d’études en vue du renforcement des capacités du personnel du MINPOSTEL en matière de cyber sécurité » a été lancé le le groupement INTEGC-KIAMA en a été adjudicataire. Ce marché porte sur quatre modules de formation dont la formation ISO 27001 Lead Auditor. Le présent document constitue le rapport de son exécution.

# **Objectifs de la formation**

## Objectif général

Maîtriser l’audit d’un système de management de sécurité de l’information (SMSI) basé sur la norme ISO/IEC 27001, en conformité avec les exigences de la norme ISO 19011 et ISO 17021.

## Objectifs spécifiques

Les participants à la formation sont désormais capables de :

* Comprendre le fonctionnement d’un Système de management de la sécurité de l’information (SMSI) conforme à la norme ISO /CEI 27001 ;
* Expliquer la corrélation entre la norme ISO/CEI 27001 et la norme ISO/CEI 27002, ainsi qu’avec d’autres normes et cadres réglementaires ;
* Comprendre le rôle d’un auditeur : planifier, diriger et assurer le suivi d’un audit de système de management conformément à la norme ISO 19011 ;
* Savoir diriger un audit et une équipe d’audit ;
* Savoir interpréter les exigences d’ISO/CEI 27001 dans le contexte d’un audit du SMSI ;
* Acquérir les compétences d’un auditeur dans le but de : planifier un audit, diriger un audit, rédiger des rapports et assurer le suivi d’un audit, en conformité avec la norme ISO 19011.

# **Méthodologie choisie**

Notre méthodologie a consisté en un cours intensif de cinq jours permettant aux participants de développer l’expertise requise pour l’audit d’un Système de Management de la Sécurité de l’Information (SMSI) et la gestion d’une équipe d’auditeurs via l’application de principes, procédures et techniques d’audit généralement reconnues.

Pendant cette formation, les participants ont acquis les aptitudes et compétences requises pour planifier et réaliser des audits internes et externes de manière efficace et conformes au processus de certification des normes ISO 19011 et ISO 17021.

Grâce aux exercices pratiques, le participant développe les aptitudes (maîtrise des techniques

d’audit) et compétences (gestion des équipes et du programme d’audit, communication avec les clients, résolution de conflits, etc.) nécessaires pour conduire efficacement un audit.

L’agenda observé est le suivant :

|  |  |  |  |
| --- | --- | --- | --- |
| **Horaire** | **Activités** | **Animateurs** | **Horaire** |
| 08h00-10h00 | Cours | Formateur | 08h00-10h00 |
| 10h00-10h30 | Pause-café | Formateur + Participants | 10h00-10h30 |
| 10h30-12h30 | Cours | Formateur | 10h30-12h30 |
| 12h30-13h30 | Pause déjeuner | Formateur + Participants | 12h30-13h30 |
| 13h30-17h00 | Cours | Formateur | 13h30-17h00 |

# **Déroulement de la formation**

La formation s’est déroulée sur une durée de 5 jours ouvrables et a débuté le lundi 22 novembre 2021 par l’installation des participants et le lancement officiel par les formateurs accompagnés de l’équipe projet de KIAMA SA.

Il a été rappelé les enjeux et les objectifs de la formation puis le matériel de formation a été distribué.

Le programme détaillé de la formation était le suivant :

|  |  |
| --- | --- |
| **Date** | **Modules dispensés** |
| Jour 1 : 22 novembre 2021 | Introduction au Système de management de la sécurité de l’information et à la norme ISO/CEI 27001   * Objectifs et structure de la formation * Cadres normatifs et règlementaires * Processus de certification * Principes fondamentaux du Système de management de la sécurité de l’information * Système de management de la sécurité de l’information |
| Jour 2 : 23 novembre 2021 | Principes, préparation et déclenchement de l’audit   * Principes et concepts fondamentaux d’audit * Approche d'audit fondée sur les preuves * Déclenchement de l’audit * Étape 1 de l’audit * Préparation de l’étape 2 de l’audit (audit sur site) * Étape 2 de l’audit (première partie) |
| Jour 3 : 24 novembre 2021 | Activités d’audit sur site   * Étape 2 de l’audit (deuxième partie) * Communication pendant l’audit h Procédures d’audit * Rédaction des plans de tests d'audit * Rédaction des constats d’audit et des rapports de non-conformité |
| Jour 4 : 25 novembre 2021 | Clôture de l’audit   * Documentation de l’audit et revue de qualité de l’audit * Clôture de l’audit * Évaluation des plans d’actions par l’auditeur * Avantages de l’audit initial * Management d’un programme d’audit interne * Compétence et évaluation des auditeurs * Clôture de la formation |
| Jour 5 : 26 novembre 2021 | Préparation pratique à l’examen de certification |

# **Domaines abordés**

Les participants ont été entretenus sur les domaines suivants :

**Domaine 1 : Principes et concepts fondamentaux de la sécurité de l’information**

Objectif principal : S’assurer que le candidat à la certification ISO/IEC 27001 Lead Auditor est en mesure de comprendre, interpréter et illustrer les principaux concepts de la sécurité de l’information relatifs au Système de Management de la Sécurité de l’Information (SMSI).

**Domaine 2 : Le Système de Management de la Sécurité de l’Information (SMSI)**

Objectif principal : S’assurer que le candidat à la certification ISO/IEC 27001 Lead Auditor est en mesure de comprendre, interpréter et illustrer les principaux concepts et composants d’un Système de Management de la Sécurité de l’Information (SMSI), en conformité avec la norme ISO/IEC 27001.

**Domaine 3 : Concepts et principes fondamentaux d’audit**

Objectif principal : S’assurer que le candidat à la certification ISO/IEC 27001 Lead Auditor est en mesure de comprendre, interpréter et appliquer les principaux concepts et les principes liés à un audit du SMSI dans le contexte de la norme ISO/IEC 27001.

**Domaine 4 : Préparation d’un audit ISO/IEC 27001**

Objectif principal : S’assurer que le candidat à la certification ISO/IEC 27001 Lead Auditor est en mesure de préparer de manière appropriée l’audit d’un SMSI dans le contexte de la norme ISO/IEC 27001.

**Domaine 5 : Conduire un audit ISO/IEC 27001**

Objectif principal : S’assurer que le candidat à la certification ISO/IEC 27001 Lead Auditor est en mesure de conduire de manière efficace un audit du SMSI dans le contexte de la norme ISO/IEC 27001.

**Domaine 6 : Clôturer un audit ISO/IEC 27001**

Objectif principal : S’assurer que le candidat à la certification ISO/IEC 27001 Lead Auditor est en mesure de clôturer un audit du SMSI et conduire des activités de suivi dans le contexte de la norme ISO/IEC 27001.

**Domaine 7 : Gérer un programme d’audit ISO/IEC 27001**

Objectif principal : S’assurer que le candidat à la certification ISO/IEC 27001 Lead Auditor est en mesure de comprendre comment établir et gérer un programme d’audit d’un SMSI.

# **Conclusion**

Le cabinet KIAMA SA, bénéficiaire du marché de renforcement des capacités du personnel du MINPOSTEL en matière de cyber sécurité a, dans cette étape réalisé le premier module portant sur la formation à la norme ISO 27001 Lead Auditor. Il était question dans cette phase du marché, d’assurer la formation de six (06) personnels du MINPOSTEL sur la norme ISO 27001 Lead Auditor. La formation s’est déroulée comme prévu, les participants ont tous répondu présents. Ils ont bénéficié des attestations officielles de fin de formation et de leur inscription pour le passage de l’examen de certification selon leur disponibilité.

Le suivi d’après formation est effectif et se déroule dans le groupe whatsapp créé à cet effet et dont le lien est le suivant : <https://chat.whatsapp.com/JsBt7Kg1qPnK97YwGZWxzV>. Dans ce groupe, les apprenants remontent les difficultés éventuelles auxquelles ils font face et son coachés en prélude à leur examen.

Le personnel formé termine cette formation, enrichi de l’expérience de l’utilisation de la norme ISO 27001. Aussi le formateur s’est assuré que ces derniers prendront le soin de bien appliquer les notions apprises dans le but d’aider le MINPOSTEL en général et la DSR en particulier à mieux réaliser ses missions.

# ANNEXES

# A1/ ATTESTATIONS DE PARTICIPATION





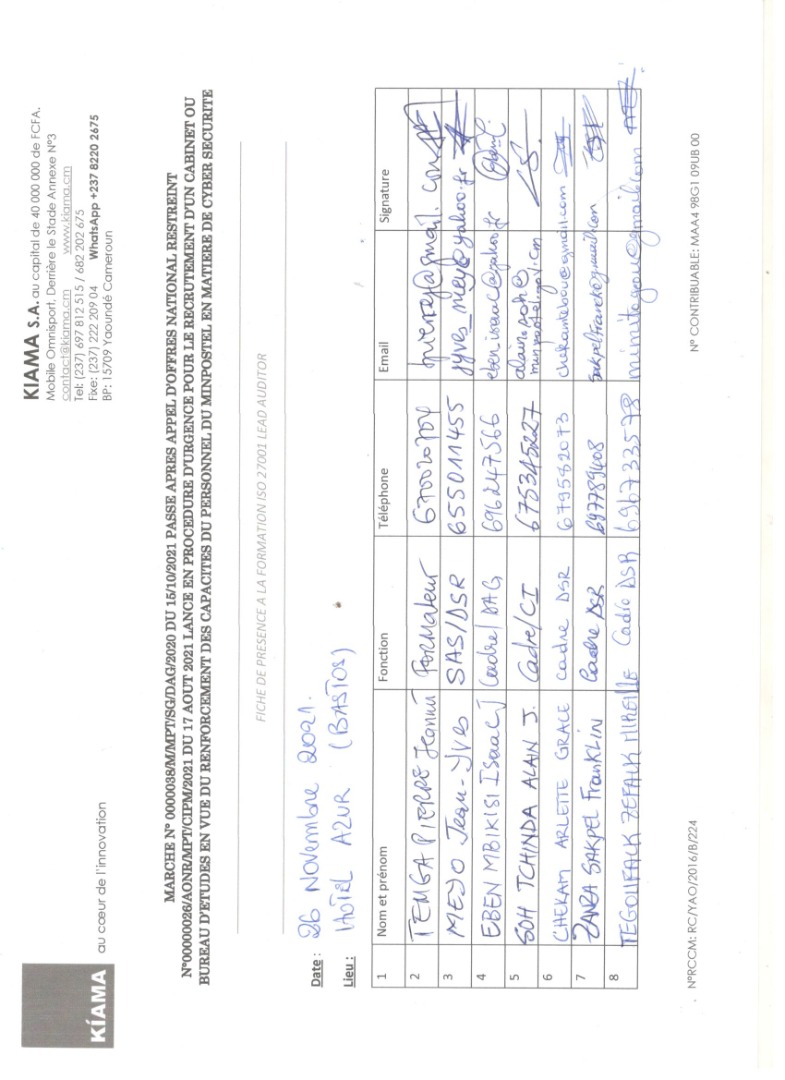
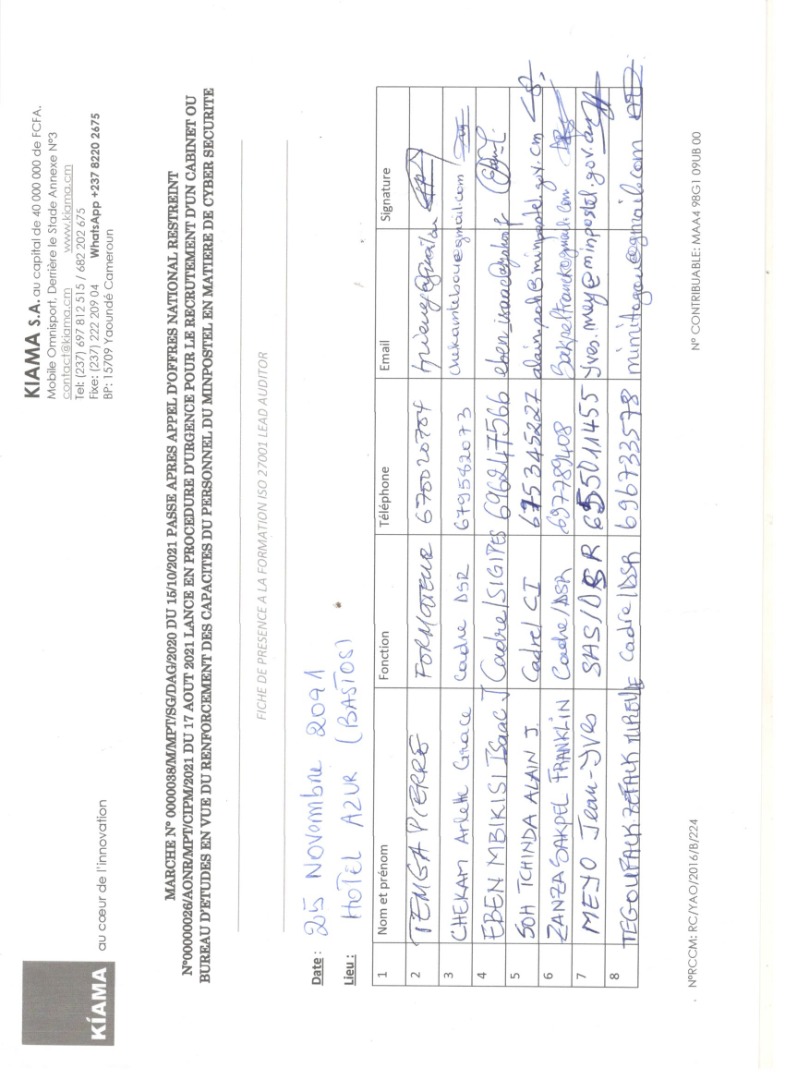
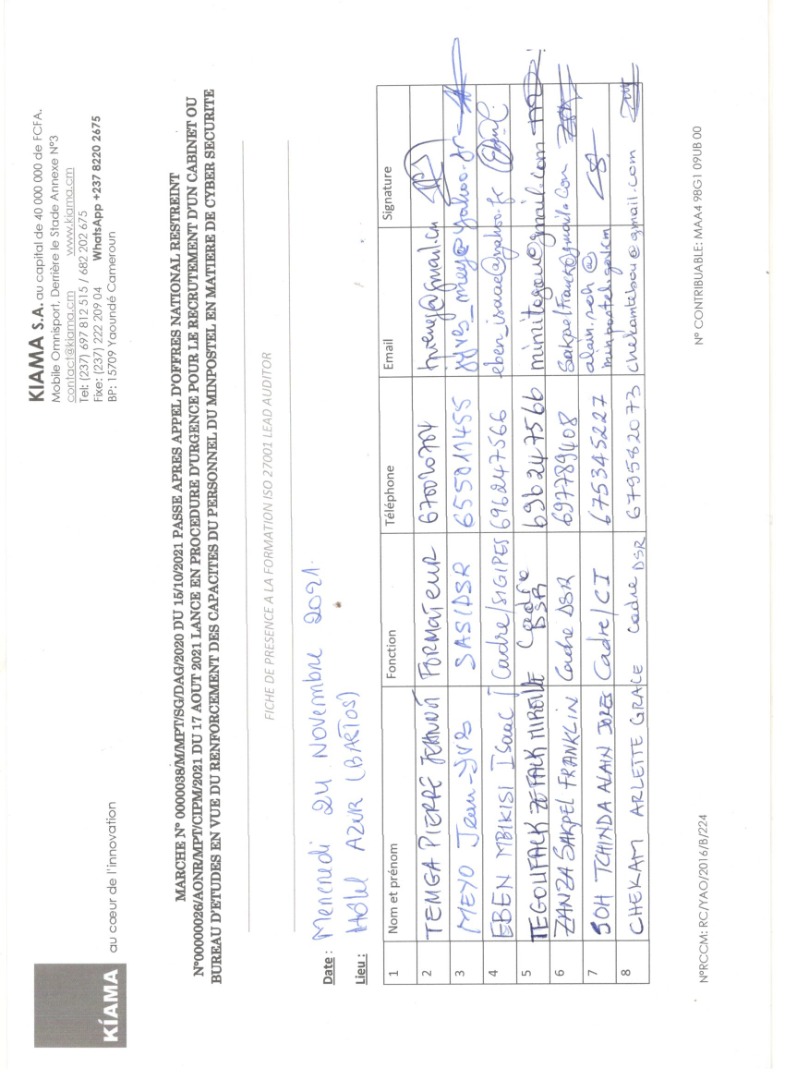
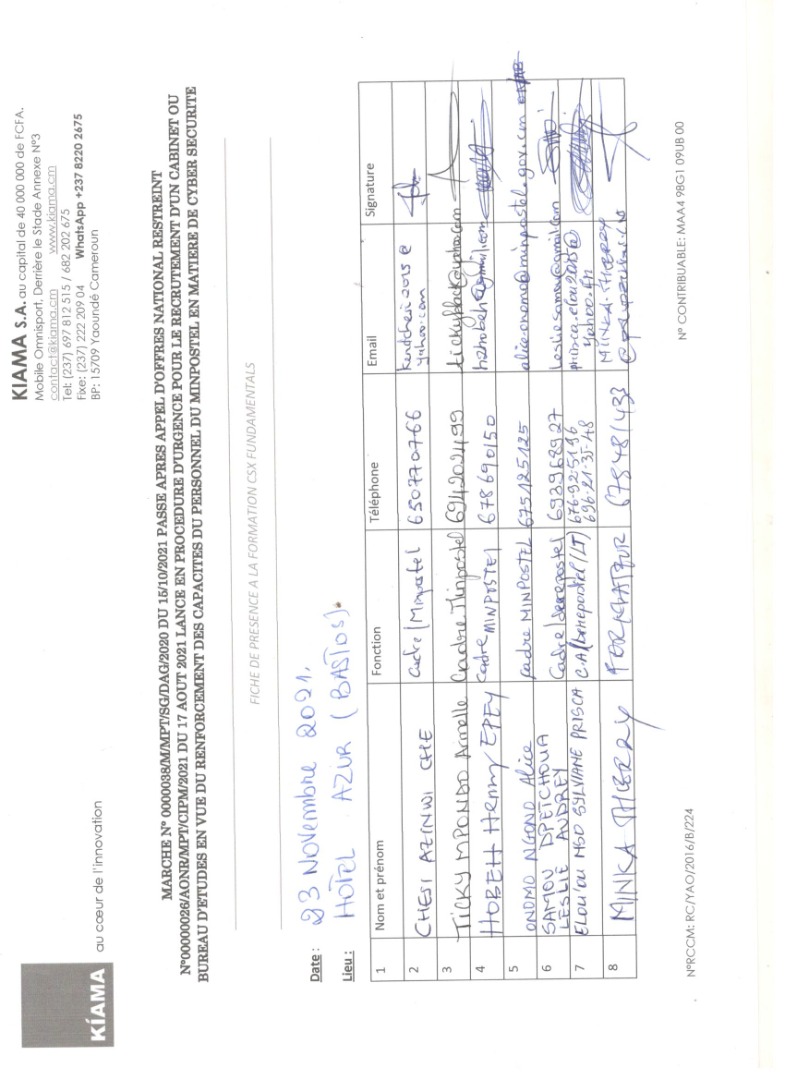
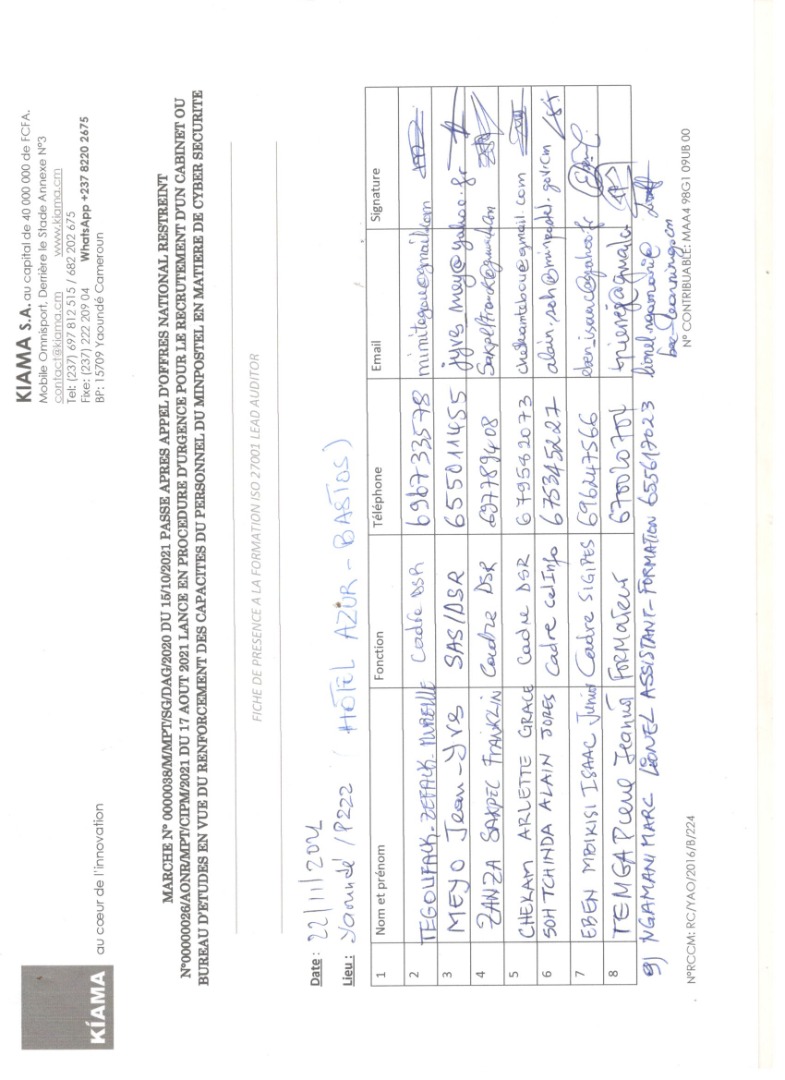








# A2/ LISTES DE PRESENCE



# A3/ PHOTOS DE FAMILLE



