Réseau des Centres d'Excellence de l'UIT pour l'Afrique

Ecole Supérieure Africaine des Technologies de l'Information et de la Communication (ESATIC)

Formation en présentielle sur la

Management de la sécurité des Systèmes d'Information (Norme ISO/IEC 27001 : Lead Implémenter)

Abidjan, Côte d'Ivoire

Du 24 au 28 février 2020

PRESENTATION DE LA FORMATION

DESCRIPTION DU COURS

Titre	**Management de la sécurité des Systèmes d'Information (Norme ISO/IEC 27001 : Lead Implémenter)**
Méthode d'enseignement	En présentiel
Objectifs	Ce cours intensif de cinq jours permet aux participants de développer l'expertise nécessaire pour accompagner une organisation dans la mise en œuvre et la gestion d'un Système de Management de la Sécurité de l'Information (SMSI) tel que spécifié dans l'ISO/CEI 27001:2013. Les participants acquerront une maîtrise des meilleures pratiques de mise en œuvre des mesures de sécurité de l´information issues des onze domaines de la norme ISO/IEC 27002. Cette formation est conforme aux bonnes pratiques de gestion de projet établies par la norme ISO 10006 (Lignes directrices pour la gestion de projet en qualité). Cette formation est aussi pleinement compatible avec les normes ISO 27003 (Lignes directrices pour l'implémentation d'un SMSI), ISO 27004 (Mesurage de la sécurité de l'information) et ISO/IEC 27005 (Gestion des risques liés à la sécurité de l'information). **Prérequis :** Une connaissance de base de la sécurité des systèmes d'information est souhaitable pour tirer un meilleur profit de cette formation.
Dates	Du 24 au 28 février 2020
Durée	5 jours
Date limite d'enregistrement	19 février 2020
Frais de formation	860 USD **Option : 860 USD (Frais de certification internationale PECB, à payer à l'ESATIC)**
Code du cours	20WS24858AFR-F

RESULTATS ATTENDUS

Aux termes de l'atelier, les auditeurs seront capables :

- de mettre en œuvre un SMSI ;
- d'expliquer les concepts, les démarches, les normes, les méthodes et les techniques nécessaires pour gérer efficacement un Système de Management de la Sécurité de l'Information ;
- d'accompagner une organisation dans la mise en œuvre, la gestion et le maintien d'un SMSI ;
- de gérer une équipe chargée de la mise en œuvre de la norme ISO/IEC 27001.

PUBLIC CIBLE

Cet atelier de formation s'adresse principalement aux profils suivants :

- Directeurs des Systèmes d'Information (DSI) ;
- Responsable de Sécurité des Systèmes d'Information (RSSI)
- responsables de projets de conformité ;
- conseillers spécialisés en technologies de l'information ;
- auditeurs internes et externes ISO/IEC 27001 ;
- membres d'équipes chargées de la sécurité de l'information.

FORMATEUR

NOM DU FORMATEUR	CONTACTS
M. PATNELLI PAUL AUGUSTE, Consultant en Conception, management, Gouvernance et Sécurité de Système d'Information. Formateur Certifié PECB	Patnellipaulauguste@gmail.com

EVALUATION

Evaluation formative;Test final

Option : Certification internationale PECB (Informations générales).

- Après avoir réussi l'examen, les participants peuvent demander la certification PECB Certified ISO/IEC 27001 Provisional Implementer, PECB Certified ISO/IEC 27001 Implementer ou PECB Certified ISO/IEC 27001 Lead Implementer, en fonction de leur niveau d'expérience.
- Un certificat sera délivré aux participants qui auront réussi l'examen et qui remplissent l'ensemble des autres exigences relatives au niveau de qualification choisi (voir le tableau ci-après).
- Les frais de certification sont inclus dans le prix de l'examen.
- Un manuel de cours contenant plus de 450 pages d'informations et d'exemples pratiques est fourni aux participants.
- Un certificat de participation de 31 crédits CPD (Continuing Professional Development) sera délivré aux participants à l'issue de la formation
- En cas d'échec, les participants peuvent repasser l'examen gratuitement, sous certaines conditions.

Certification	Examen	Expérience professionnelle	Expérience d'audit SMSI	Expérience de projet SMSI	Autres exigences
PECB Certified ISO/IEC 27001 Provisional Implementer	Examen PECB Certified ISO/IEC 27001 Lead Implementer	Aucune	Aucune	Aucune	Signer le code d'éthique du PECB
PECB Certified ISO/IEC Implementer	Examen PECB Certified ISO/IEC 27001 Lead Implementer	Deux années Dont une année d'expérience en sécurité de l'information	Aucune	Activités totalisant 200 heures	Signer le code d'éthique du PECB
PECB Certified ISO/IEC 27001 Lead Implementer	Examen PECB Certified ISO/IEC 27001 Lead Implementer	Cinq années deux années d'expérience en sécurité de l'information	Aucune	Activités totalisant 300 heures	Signer le code d'éthique du PECB

AGENDA

Date du 1er jour	Heure de début, Heure de fin	Sujets / Activités
24/02/2020	09 :00 - 09 :30	Accueil, enregistrement et ouverture du séminaire.
	Session du matin (09 :30 - 12 :45)	**Introduction (1)** ▪ Introduction aux systèmes de management et à l'approche processus. ▪ Présentation de la suite des normes ISO/IEC 27000 ainsi que du cadre normatif, légal et réglementaire.
	Session du matin (09 :30 - 12 :45)	**Introduction (2)** ▪ Principes fondamentaux de la sécurité de l'information. ▪ Analyse préliminaire et détermination du niveau de maturité d'un système de management de sécurité de l'information existant d'après l'ISO 21827. ▪ Rédaction d'une étude de faisabilité et d'un plan projet pour la mise en œuvre d'un SMSI.
Date du 2ième jour	**Heure de début, Heure de fin**	**Sujets / Activités**
25/02/2020	Session du matin (09:00 – 12:15)	**Planification de la mise en œuvre d'un SMSI basé sur la norme ISO/IEC 27001 (1)** ▪ Définition du périmètre (domaine d'application) du SMSI. ▪ Développement d'un SMSI et des politiques de sécurité de l'information. ▪ Sélection de l'approche et de la méthode d'appréciation des risques.

	Session de l'après-midi (13:45 - 17:00)	**Planification de la mise en œuvre d'un SMSI basé sur la norme ISO/IEC 27001 (2)** ▪ Gestion des risques : identification, analyse et traitement du risque (selon la norme ISO/IEC 27005). ▪ Rédaction de la déclaration d'applicabilité.
Date du 3ième jour	**Heure de début, Heure de fin**	**Sujets / Activités**
26/02/2020	Session du matin (09:00 – 12:15)	**Mise en œuvre d'un SMSI conforme à la norme ISO/IEC 27001 (1)** ▪ Mise en œuvre d'un cadre de gestion documentaire. ▪ Élaboration et mise en œuvre des contrôles de sécurité. ▪ Formation, sensibilisation et communication.
	Session de l'après-midi (13:45 - 17:00)	**Mise en œuvre d'un SMSI conforme à la norme ISO/IEC 27001 (2)** ▪ Gestion des incidents (selon la norme ISO 27035). ▪ Gestion des opérations d'un SMSI.
Date du 4ième jour	**Heure de début, Heure de fin**	**Sujets / Activités**
27/02/2020	Session du matin (09:00 – 12:15)	**Contrôler, surveiller, mesurer et améliorer un SMSI, en conformité avec la norme ISO/IEC 27001 (1)** ▪ Contrôler les mesures de sécurité du SMSI. ▪ Développement de mesures, d'indicateurs de performance et de tableaux de bord conformes à la norme ISO 27004. ▪ Audit interne ISO/IEC 27001.
	Session de l'après-midi (13:45 - 17:00)	**Contrôler, surveiller, mesurer et améliorer un SMSI, en conformité avec la norme ISO/IEC 27001 (2)** ▪ Revue de direction du SMSI. ▪ Amélioration continue. ▪ Préparation à l'audit de certification ISO/IEC 27001.
Date du 5ième jour	**Heure de début, Heure de fin**	**Sujets / Activités**
28/02/2020	Session du matin (09:00 – 12:15)	Evaluation des auditeurs (Examen de certification internationale PECB)
	Session de l'après-midi (12 :15 - 13 :30)	Evaluation du séminaire et clôture de l'atelier.

METHODOLOGIE

Exposés, travaux pratiques, étude de cas et échanges interactifs.

COORDINATION DE LA FORMATION

Coordinateur de la formation : Nom : KOSSONOU Rodolphe Chef du Service de la Formation Continue, ESATIC Tel. : + 225 21 218 100 Fax : + 225 51 400145 Email : rodolphe.kossonou@esatic.edu.ci	**Coordinateur de l'UIT :** Nom : Elena Stankovska-Castilla Tel : +41 22 730 60 27 Email: elena.stankovska-castilla@itu.int; hcbmail@itu.int

INSCRIPTION ET PAIEMENT

Inscription sur le portail de l'ITU Académie :
L'inscription et le paiement doivent se faire en ligne sur le portail web de l'ITU Académie. Afin de pouvoir vous inscrire à un cours vous **devez** au préalable créer un compte sur le portail web d'ITU Académie à l'adresse suivante :
https://academy.itu.int/index.php/user/register
Inscription à une formation :

Si vous avez déjà un compte ou que vous créez un nouveau compte, vous pouvez vous inscrire en ligne pour la formation à l'adresse suivante :
https://academy.itu.int/training-courses/full-catalogue/management-de-la-securite-des-systemes-dinformation-norme-isoiec-27001-lead-implementer

Vous pouvez également vous inscrire en trouvant le cours qui vous intéresse dans notre catalogue de formation
https://academy.itu.int/index.php/training-courses/full-catalogue

Paiement

1. Paiement en ligne

Les frais de participation à cette formation sont de **860 USD**. Ce montant prend en compte l'inscription, la documentation, la pause-café et le déjeuner. Il est recommandé de procéder au paiement via le système de paiement en ligne en utilisant le même lien que celui de l'inscription en ligne :
https://academy.itu.int/training-courses/full-catalogue/management-de-la-securite-des-systemes-dinformation-norme-isoiec-27001-lead-implementer

2. Paiement par virement bancaire

Lorsqu'il n'est pas possible d'effectuer un paiement via le système en ligne, sélectionnez l'option de paiement hors ligne ''offline'' pour générer une facture en utilisant le même lien que ci-dessus. Téléchargez la facture pour effectuer un virement sur le compte bancaire de l'UIT indiqué ci-dessous. Envoyez ensuite la preuve de paiement / la copie du bordereau de virement et la copie de la facture à Hcbmail@itu.intet mettre en copie le coordinateur du cours. **Tous les frais de transaction bancaire doivent être à la charge du payeur**.
Si les documents ci-dessus ne sont pas soumis, le candidat pourrait ne pas être inscrit à la formation.

3. Paiement par groupe

Si vous souhaitez payer pour plus d'un participant par virement bancaire et que vous avez besoin d'une facture pour tous, créez un compte comme **contact institutionnel.** Les contacts institutionnels sont des utilisateurs qui représentent une organisation. Tout étudiant peut demander à être un contact institutionnel ou à appartenir à une organisation existante.

Pour ce faire, accédez à la page de votre profil en cliquant sur le bouton **"My account"** dans le menu de l'utilisateur. Au bas de cette page, vous devriez voir deux boutons :

a. Si vous souhaitez **devenir un contact institutionnel**, cliquez sur le bouton "**Apply to be an Institutional Contact"**. Cela vous redirigera vers un petit formulaire qui vous demandera le nom de l'organisation. Une fois que vous avez renseigné le nom de l'organisation que vous souhaitez représenter, cliquez sur **"continue",** une demande est alors créée. Un responsable de l'Académie de l'UIT examinera manuellement cette demande et l'acceptera ou la refusera en conséquence.

b. Si vous souhaitez **appartenir à une organisation existante**, cliquez sur le bouton **"Request to belong to an Institutional Contact"**. Cela vous redirigera vers un petit formulaire qui vous demandera de sélectionner l'organisation à laquelle vous souhaitez appartenir à partir d'une liste d'organisations. Après avoir sélectionné la bonne organisation et cliqué sur **"continue"**, une demande sera créée. Le contact institutionnel qui représente cette organisation acceptera ou refusera manuellement votre demande d'adhésion à l'organisation.

Coordonnées bancaires de l'UIT :	
Nom et addresse de la Banque :	UBS SWITZERLAND AG Case postale 2600 CH 1211 Geneva 2 Switzerland
Beneficiaire:	Union Internationale des Télécommunications
Numero de Compte :	240-C8108252.2 (USD)
Swift:	UBSWCHZH80A
IBAN	CH54 0024 0240 C810 8252 2
Montant :	860 USD
Reference du paiement :	CoE-AFR 24858 - P.40590.1.04

4. Autres méthodes de paiement

Si pour des raisons de régulations nationales il y a des restrictions ne permettant pas d'utiliser les options de paiement 1 et 2 ci-dessus, veuillez contacter le coordinateur de l'UIT pour plus d'assistance.