



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 présentielle sur la
Gestion des Risques en Entreprise

Abidjan, Côte d'Ivoire
20 au 24 mai 2019

PRESENTATION DE LA FORMATION

DESCRIPTION DU COURS

Titre	Gestion des risques en entreprise
Objectifs	<p>La gestion des risques en entreprise est le fondement d'une saine gestion et d'une gouvernance efficace des diverses ressources. En outre, elle est encadrée par des règlements et des normes internationales comme les normes ISO 32000 et ISO 27005. Être en mesure d'identifier les risques constitue l'une des premières étapes dans la gestion des risques en entreprise qui vise à déployer les actions nécessaires pour mieux les gérer au lieu de subir, voir même les éviter au lieu de les avoir.</p> <p>Alliant théorie et aspects pratiques, cette formation de 5 jours aide les participants à comprendre la gestion des risques en entreprise, à savoir appliquer les principes et les bonnes pratiques qui s'y rattachent et à les initier aux principes fondamentaux de la gestion des risques liés à :</p> <ul style="list-style-type: none">▪ la gestion des projets ;▪ la sécurité des systèmes d'information ;▪ la protection des données à caractère personnel. <p>Prérequis : Connaissances générales de la sécurité des systèmes d'information</p>
Dates	Du 20 au 24 mai 2019
Durée	5 jours
Date limite d'enregistrement	15 mai 2019
Frais de formation	860 USD
Code du cours	19WS24304AFR-F

RESULTATS ATTENDUS

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

- identifier les risques et de réagir de façon efficace ;
- faire une étude simplifiée et exhaustive des divers risques ;
- comprendre le processus de gestion des risques et les objectifs à atteindre ;
- maîtriser les approches et les méthodologies de gestion des risques: EBIOS, MEHARI, OCTAVE,... ;
- améliorer la prise de décision, la planification et la priorisation des divers risques ;
- mettre en place les mesures nécessaires pour anticiper et prévenir face aux divers risques ;
- savoir traiter les divers risques liés à la gestion des projets, au système d'information et à la protection des données à caractère personnel ;
- déterminer les coûts et les bénéfices associés à la gestion des risques ;
- maîtriser et apprendre à implémenter les normes ISO 32000 et ISO 27005.

PUBLIC CIBLE

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

- Directeurs des systèmes d'information (DSI) ;
- Responsables de sécurité des systèmes d'information (RSSI) ;
- Gestionnaires des risques (Risk Manager) ;
- Consultants, experts et auditeurs en sécurité ;
- Enseignants, chercheurs et étudiants en sécurité.

FORMATEUR

NOM DU FORMATEUR	CONTACTS
Nizar Ben Neji est un expert en Cyber sécurité ayant 15 ans d'expérience dans des projets de grandes envergures, la formation et l'animation de séminaires sur divers thèmes en relation avec la cybersécurité et la cybercriminalité. Nizar Ben Neji est un Docteur en Technologie de l'Information et de la Communication (TIC) de l'université de Carthage. Il est également un expert travaillant avec l'UIT (Union Internationale des Télécommunications), la CTO (Commonwealth Telecom Organization) et l'AICTO (Organisation Arabe des Technologies de l'Information et des Télécommunications).	nizar.benneji@fsb.rnu.tn / nizarbenneji@gmail.com (+216) 99 207 377

EVALUATION

Evaluation théorique à travers un questionnaire à choix multiple

AGENDA

1 ^{er} jour – 20 mai	Heure de début, Heure de fin	Sujets/Activités
	09:00 - 09:30	Accueil, enregistrement et ouverture du séminaire.
	Session du matin (09:30 - 12:45)	Introduction à la gestion des risques <ul style="list-style-type: none">▪ Définition d'un risque▪ Divers types de risques▪ Vocabulaire du management du risque

		<ul style="list-style-type: none"> ○ Danger ○ Probabilité d'occurrence ou fréquence ○ Gravité ○ Acceptabilité ○ Facteur de risque ○ Impact ○ Capitalisation ○ Gestionnaire du risque ▪ Domaines d'application de la gestion des risques <ul style="list-style-type: none"> ○ Gestion des projets ○ Sécurité des SI ○ Protection de la vie privée ○ ... ▪ Référentiels et méthodologies de gestion des risques
	Session de l'après-midi (14:00 - 17:15)	<p><u>Processus de gestion des risques</u></p> <ul style="list-style-type: none"> ▪ Identification ▪ Appréciation ▪ Traitement <ul style="list-style-type: none"> ○ réduction, maintien, refus et partage du risque ○ risque actuel et résiduel ▪ Suivi et réaction en cas de problèmes
2^{ème} jour – 21 mai	Heure de début, Heure de fin	Sujets/Activités
	Session du matin (09:00 – 12:15)	<p><u>Gestion de risque en gestion de projet (1/2)</u></p> <ul style="list-style-type: none"> ▪ Conduction d'un projet ▪ Clarification des objectifs du projet ▪ Clarification des ressources du projet <ul style="list-style-type: none"> ○ Ressources humaines ○ Ressources matérielles et logicielles ○ Financement ○ Temps ▪ Processus de gestion de risques : <ul style="list-style-type: none"> ○ Identification exhaustive des risques menaçants les ressources du projet ○ Analyse et évaluation de la criticité des risques et définition des priorités ○ Etablissement d'un plan de prévention, de maîtrise et de traitement des risques ▪ Menaces en gestion de projet : <ul style="list-style-type: none"> ○ Menaces liées au facteur humain ○ Menaces liées aux ressources temporelles

		<ul style="list-style-type: none"> ○ Menaces liées à l'infrastructure matérielle et logicielle, au cadre et à l'environnement du projet ○ Menaces liées au financement
	<p>Session de l'après-midi (13:45 - 17:00)</p>	<p><u>Gestion des risques en gestion de projets (2/2)</u></p> <ul style="list-style-type: none"> ▪ Démarche d'identification des risques <ul style="list-style-type: none"> ○ Exploitation de la documentation et des outils de gestion de projet ○ Réunion de brainstorming et implication des divers acteurs ○ Questionnaire et interview sur la base des lignes directrices des normes ○ Capitalisation sur les expériences passées ▪ Priorisation des risques <ul style="list-style-type: none"> ○ Fréquence/Gravité ○ Difficulté de détection ○ Criticité ○ Matrice des risques ▪ Traitement des risques <ul style="list-style-type: none"> ○ Mesures de protection ○ Mesures préventives ○ Mesures techniques ○ Mesures juridiques ○ Mesures organisationnelles ○ Mesures financières ▪ Plan de traitement des risques <ul style="list-style-type: none"> ○ Analyse des causes ○ Diagramme causes-effet ○ Risques multifactoriels ○ Structuration du plan de traitement des risques ▪ Suivi des risques <ul style="list-style-type: none"> ○ Réactivité / Proactivité ○ Matriced'Eisenhower ○ Déléguer, réaliser, éliminer et planifier les tâches de traitement des risques
3^{ème} jour – 22 mai	Heure de début, Heure de fin	Sujets / Activités
	<p>Session du matin (09:00 – 12:15)</p>	<p><u>Gestion des risques de sécurité des systèmes d'information</u></p> <ul style="list-style-type: none"> ▪ Classes des vulnérabilités ▪ Référentiels OWASP des vulnérabilités Web, Cloud, Mobile et IoT ▪ Types des menaces (accidentelles et intentionnelles)

		<ul style="list-style-type: none"> ▪ Divers formes d'attaques sur les systèmes d'information <ul style="list-style-type: none"> ○ Active/Passive ○ Interne/Externe ▪ Risques de sécurité sur les systèmes d'information des entreprises
	Session de l'après-midi (13:45 - 17:00)	<p><u>Normes et méthodologies de gestion des risques de sécurité</u></p> <ul style="list-style-type: none"> ▪ Norme ISO/IEC 27005 ▪ Méthodologie EBIOS ▪ Méthodologie MEHARI
4^{ème} jour – 23 mai	Heure de début, Heure de fin	Sujets / Activités
	Session du matin (09:00 – 12:15)	<p><u>Gestion des risques de sécurité selon la norme 27005</u></p> <ul style="list-style-type: none"> ▪ Etablissement du contexte ▪ Appréciation, analyse et estimation des risques ▪ Evaluation des risques et prise de décision ▪ Définition du plan de traitement des risques
	Session de l'après-midi (13:45 - 17:00)	<p><u>Gestion des risques sur la vie privée (1/2)</u></p> <ul style="list-style-type: none"> ▪ Définition des données à caractère personnel (DCP) ▪ Risques sur la vie privée <ul style="list-style-type: none"> ○ Gravité ○ Vraisemblance ○ Niveau de risque ▪ Eléments à protéger ▪ Evènements redoutables : <ul style="list-style-type: none"> ○ Indisponibilité des processus du traitement ○ Modification des processus de traitement ○ Accès illégitime aux DCP ○ Modification non désirée des DCP ○ Disparition des DCP ▪ Sources de risque <ul style="list-style-type: none"> ○ Personnes internes à l'organisme ○ Personnes externes ○ Sources non humaines ▪ Supports à protéger <ul style="list-style-type: none"> ○ Matériels ○ Logiciels ○ Canaux de transmission informatique ○ Personnes ○ Supports papier ○ Canaux de transmission papier

5 ^{ème} jour – 24 mai	Heure de début, Heure de fin	Sujets / Activités
	Session du matin (09:00 – 12:15)	<p><u>Gestion des risques sur la vie privée (2/2)</u></p> <ul style="list-style-type: none"> ▪ Démarche EBIOS pour la gestion des risques sur la vie privée : <ul style="list-style-type: none"> ○ le contexte du traitement considéré, ○ les événements redoutés dans ce contexte, ○ les menaces envisageables (si besoin), ○ les risques qui en découlent (si besoin), ○ les mesures appropriées pour les traiter. <p>Evaluation des auditeurs</p>
	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

<p>Coordinateur de la formation: Nom : Rodolphe Kossonou Chef du Service de la Formation Continue, ESATIC Tel. : + 225 21 218 100 Fax : + 225 51 400 145 Email : rodolphe.kossonou@esatic.ci</p>	<p>Coordinateur de l'UIT: Nom : Elena Stankovska-Castilla Tel: +41 22 730 60 27 E-mail : elena.stankovska-castilla@itu.int</p>
---	---

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/index.php/training-courses/full-catalogue/gestion-des-risques-en-entreprise>

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>

Païement

1. Païement 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/index.php/training-courses/full-catalogue/gestion-des-risques-en-entreprise>

2. Païement 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.int et 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. Païement de 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 "**Mon compte**" dans le menu de l'utilisateur. Au bas de cette page, vous devriez voir deux boutons :

- Si vous souhaitez **devenir un contact institutionnel**, cliquez sur le bouton "**Postuler pour être un contact institutionnel**". 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 « **Continuer** », 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.
- Si vous souhaitez **appartenir à une organisation existante**, cliquez sur le bouton "**Demander à appartenir à un contact institutionnel**". 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 « **Continuer** », 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 adresse de la Banque :	UBS SWITZERLAND AG Case postale 2600 CH 1211 Geneva 2 Switzerland
Bénéficiaire:	Union Internationale des Télécommunications
Numéro de compte:	240-C8108252.2 (USD)
Swift:	UBSWCHZH80A
IBAN	CH54 0024 0240 C810 8252 2
Montant :	860 USD
Référence du paiement :	CoE-AFR 24304 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.