



Plan du cours

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

Titre	Gestion des risques liés à la sécurité de l'information (Norme ISO/IEC 27005: Risk manager)
Modalité de la formation	Formation en ligne par un formateur
Dates	Du 9 au 21 mai 2022
Durée	02 semaines
Date limite d'enregistrement	2 mai 2022
Frais de formation	50 USD / 30 000 F CFA (XOF et XAF)
Description	Cette formation met l'accent sur: <ul style="list-style-type: none">– La compréhension des concepts, approches et méthode de la gestion des risques de la sécurité de l'information ;– les exigences de la norme ISO/IEC 27001 dans le cadre de la gestion des risques de la sécurité de l'information.– la connaissance des meilleures pratiques en matière de gestion des risques liés à la sécurité de l'information.
Code de la formation	22OI28045AFR-F

1.OBJECTIFS D'APPRENTISSAGE

Cet atelier permet aux participants de développer les compétences pour maîtriser les éléments de base du management du risque liés à tous les actifs pertinents de la sécurité de l'information en utilisant la norme ISO/IEC 27005 comme cadre de référence. Grâce aux exercices pratiques et aux études de cas, le participant pourra acquérir les connaissances et les compétences pour réaliser une appréciation optimale du risque de la sécurité de l'information et pour gérer les risques à temps en prenant connaissance de leur cycle de vie. Pendant cette formation nous présenterons également d'autres méthodes d'appréciation du risque comme OCTAVE, EBIOS, MEHARI et Harmonized TRA. Cette formation correspond parfaitement au processus de mise en œuvre du cadre du SMSI de la norme ISO/IEC 27001 .

2.RESULTATS ATTENDUS

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

- comprendre la relation entre la gestion des risques de la sécurité de l'information et les mesures de sécurité ;
- comprendre les concepts, approches, méthodes et techniques permettant un processus de gestion des risques efficace et conforme à ISO/IEC 27005 ;

- savoir interpréter les exigences de la norme ISO/IEC 27001 dans le cadre de la gestion des risques de la sécurité de l'information ;
- acquérir les compétences pour conseiller efficacement les organisations sur les meilleures pratiques en matière de gestion des risques liés à la sécurité de l'information.

3. PUBLIC CIBLE

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

- Responsables de la sécurité d'information ;
- Membres d'une équipe de sécurité de l'information ;
- Tout personne responsable de la sécurité d'information, de la conformité et du risque dans une organisation ;
- Toute personne mettant en œuvre ISO/CEI 27001, désirant se conformer à la norme ISO/CEI 27001 ou impliqué dans un programme de gestion des risques ;
- Consultants des TI (Technologies de l'information) ;
- Professionnels des TI (Technologies de l'information) ;
- Agents de la sécurité de l'information ;
- Agents de la protection des données personnelles.

4. CONDITIONS D'ENTREE

Des connaissances fondamentales en sécurité informatique et une connaissance préalable de la norme ISO/IEC 27001 sont utiles pour suivre cette formation et en tirer un meilleur profit.

5. FORMATEURS/INSTRUCTEURS

NOM DU FORMATEUR	CONTACTS
M. KONATE TIORNON, Formateur Certifié PECB ISO/IEC 27005 : Risk manager Consultant : conception, management, Gouvernance et Sécurité de Système d'Information , ingénierie pédagogique.	tiornon@gmail.com

6. CONTENU DU COURS

- I. Concepts et définitions liés au management du risque**
- II. Programme du management du risque selon l'ISO/IEC 27005**
 - Normes, cadres et méthodologies du management du risque.
 - Mise en œuvre d'un programme de management du risque de la sécurité de l'information
 - Comprendre l'organisation et son contexte
- III. Identification, appréciation, évaluation, traitement, acceptation, communication et surveillance du risque selon l'ISO/IEC 27005**
 - Identification du risque
 - Analyse et évaluation du risque
 - Appréciation du risque avec une méthode quantitative
 - Traitement du risque
 - Acceptation du risque et management des risques résiduels
 - Communication et consultation concernant le risque de la sécurité de l'information
 - Surveillance du risque et revue
- IV. Aperçu général des autres méthodes d'appréciation du risque de la sécurité de l'information**
 - Présentation de la méthode OCTAVE

- Présentation de la méthode MEHARI
- Présentation de la méthode EBIOS
- Présentation de la méthode Harmonized TRA

7. AGENDA DU COURS

Jours	Activités	Exercices et interactions
Jour 1 et 2 (28 février et 01 mars 2022)	Concepts et définitions liés au management du risque	Cours disponible en ligne Quizz d'auto-évaluation 1 Discussion en ligne d'une heure le 01 mars 2022 (de 18h00 à 19h00 GMT)
Jour 3 et 4 (02 et 03 mars 2022)	<u>Identification, appréciation, évaluation, traitement, acceptation, communication et surveillance du risque selon l'ISO/IEC 27005 (1)</u> <ul style="list-style-type: none"> ▪ Identification du risque ▪ Analyse et évaluation du risque ▪ Appréciation du risque avec une méthode quantitative ▪ Traitement du risque 	Cours disponible en ligne Quizz d'auto-évaluation 2 Discussion en ligne d'une heure le 03 mars 2022 (de 18h00 à 19h00 GMT)
Jour 5 et 6 (04 et 05 mars 2022)	<u>Identification, appréciation, évaluation, traitement, acceptation, communication et surveillance du risque selon l'ISO/IEC 27005 (2)</u> <ul style="list-style-type: none"> ▪ Acceptation du risque et management des risques résiduels ▪ Communication et consultation concernant le risque de la sécurité de l'information ▪ Surveillance du risque et revue 	Cours disponible en ligne Quizz d'auto-évaluation 3 Discussion en ligne d'une heure le 05 mars 2022 (de 18h00 à 19h00 GMT)
Jour 7 et 8 (07 et 08 mars 2022)	<u>Aperçu général des autres méthodes d'appréciation du risque de la sécurité de l'information (1)</u> <ul style="list-style-type: none"> ▪ Présentation de la méthode OCTAVE ▪ Présentation de la méthode MEHARI 	Cours disponible en ligne Quizz d'auto-évaluation 4 Discussion en ligne d'une heure le 08 mars 2022 (de 18h00 à 19h00 GMT)
Jour 9 et 10 (09 et 10 mars 2022)	<u>Aperçu général des autres méthodes d'appréciation du risque de la sécurité de l'information (2)</u> <ul style="list-style-type: none"> ▪ Présentation de la méthode EBIOS ▪ Présentation de la méthode Harmonized TRA 	Cours disponible en ligne Quizz d'auto-évaluation 5 Discussion en ligne d'une heure le 10 mars 2022 (de 18h00 à 19h00 GMT)
Jour 11 (12 mars 2022)	Evaluation des participants et clôture de la formation.	Quizz final

8. MODE D'ANIMATION PEDAGOGIQUE

Cette formation se déroulera sur une période de deux semaines avec environ trois (3) leçons par semaine et un pré-test le premier jour.

Ce cours est entièrement à distance (en ligne), grâce aux supports de cours disponibles, vous allez acquérir ou améliorer vos compétences afin de gérer un programme de gestion des risques en sécurité de l'information, tout en bénéficiant des échanges de la communauté sur le forum de discussion.

Des travaux pratiques, études de cas seront mis à la disposition des auditeurs. Des exercices d'auto-évaluation, des quiz de fin de leçon permettront d'évaluer vos acquis. Des réunions en ligne d'une heure seront animées par le formateur pour discuter de manière interactive sur les contenus.

Un Quiz final sera mis à la disposition des auditeurs à la fin de l'atelier.

9. EVALUATION ET NOTATION

Un Quizz final sous forme de questions QCM sera mis à la disposition des participants à la fin de l'atelier.

Pour obtenir le certificat délivré par l'ESATIC et l'UIT au terme de la formation, vous devez avoir un score moyen égal ou supérieur à 60%.

COORDINATION DU COURS

Coordonnateur du centre d'excellence: Nom: KOSSONOU Rodolphe Titre : Chef du Service de la Formation Continue Tel : + 225 01 51 400 145 Email: rodolphe.kossonou@esatic.edu.ci	Coordinateur UIT: Nom : M. Emmanuel Niyikora Responsable de Programme, bureau de zone UIT pour l'Afrique de l'Ouest, Dakar Tel : +250 788312939 Email: (emmanuel.niyikora@itu.int)
--	---