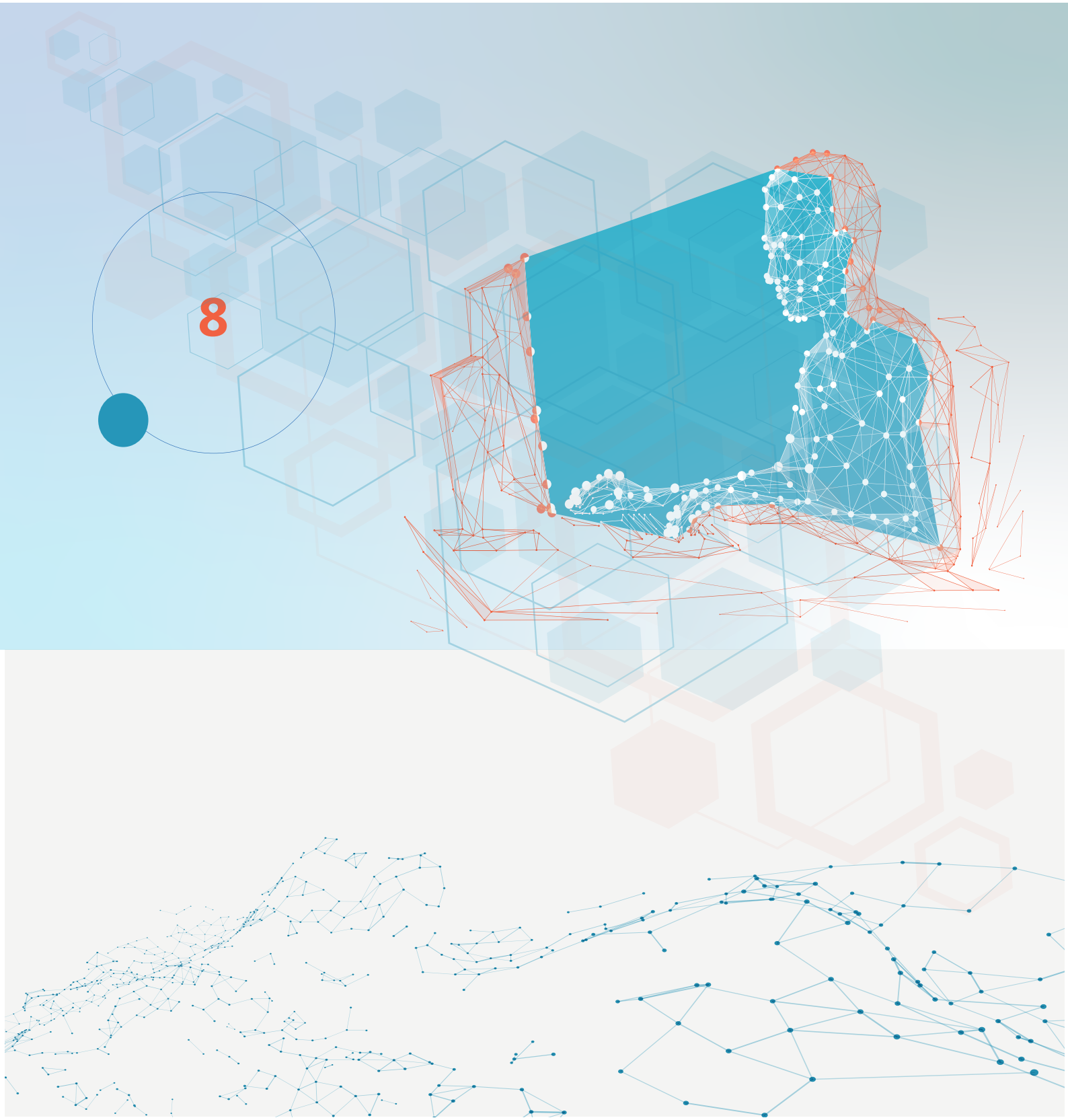
8



8. Préparation à la certification ISO 27005 Risk Manager

OBJECTIFS DE LA FORMATION

L' objectif de cette formation est de :

- 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 du management du risque de la sécurité de l'information
- Acquérir les compétences pour conseiller efficacement les organisations sur les meilleures pratiques en matière de management du risque lié à la sécurité de l'information

La durée de la formation est de 4 jours.

CONTENU DE LA FORMATION

Jour 1 : Introduction à la norme ISO/IEC 27005 et à la mise en oeuvre d'un programme de gestion des risques

Les différents points qui seront traités sont les suivants :

Section 1 : Objectifs et structure de la formation ;
Section 2 : Cadres normatifs et réglementaires ;
Section 3 : Concepts et définitions du risque ;
Section 4 : Programme de gestion des risques ;
Section 5 : Etablissement du contexte.

Jour 2 : Introduction à la norme ISO/IEC 27005 et à la mise en oeuvre d'un programme de gestion des risques

Les différents points qui seront traités sont les suivants :

Section 6 : Identification des risques ;
Section 7 : Analyse des risques ;
Section 8 : Evaluation des risques ;
Section 9 : Appréciation des risques à l'aide d'une méthode quantitative ;
Section 10 : Traitement des risques ;
Section 11 : Acceptation des risques en sécurité de l'information.

8. Préparation à la certification ISO 27005 Risk Manager (Suite et fin)

Jour 3 : Communication, consultation, surveillance, revue des risques et méthodes d'appréciation des risques

Les différents points qui seront traités sont les suivants :

Section 12 : Communication et concertation relatives aux risques en sécurité de l'information ;
Section 13 : Surveillance et réexamen des risques en sécurité de l'information ;
Section 14 : Méthode OCTAVE ;
Section 15 : Méthode MEHARI ;
Section 16 : Méthode EBIOS ;
Section 17 : Méthode harmonisée d'évaluation des menaces et des risques (EMR) ;
Section 18 : Processus de certification et clôture de la formation.

Jour 4 : Révisions et Examen de certification

Les examens sont payants pour toute certification et leur coût n'est pas compris dans le prix de la formation. Ils seront faits en ligne.

FORMAT

La formation se passe sous forme de présentation Powerpoint, d'interactions entre les participants et le formateur et d'ateliers pratiques entre les participants.

INTERVENANT

Aamadou Moctar BA

Expert SI & Sécurité SI, Formateur agréé PECB, le Formateur participe à des missions de conseil et d'assistance, de pilotage de projets de système d'information et sécurité informatique (Implémentation SMSI, audit/diagnostic, plan stratégique SI, Schéma directeur SI, transformation digitale, etc.). Par ailleurs, le Formateur est titulaire de Lead Implementer / Auditor ISO 27001, Risk Manager ISO 27005, Lead Application Security Implementer ISO 27034 et anime des formations à la sécurité des SI, gestion des risques, sécurité des applications et cybersécurité.