DIGITAL ACT®
ACADEMY

ISO 27032

ISO 27032 Lead Cybersecurity Manager

1. Présentation

Aujourd'hui plus que jamais, l'émergence des nouvelles technologies digitales a profondément transformé le quotidien des organisations et des personnes. La sécurité du cyberespace n'est pas en reste car les menaces ne cessent d'augmenter.

Dans ce contexte, la cybersécurité est un enjeu de taille car elle se doit de protéger la vie privée, l'intégrité et l'accessibilité des données dans le cyberespace.

Publiée en juillet 2012, la norme internationale ISO/IEC 27032 vise à mettre l'accent sur le rôle des différentes sécurités dans le cyberespace en matière d'informations, de réseaux, de l'Internet et de la protection des infrastructures critiques.

A travers une session de cinq (5) jours, les participant(e)s pourront développer les compétences nécessaires pour accompagner une organisation dans la mise en œuvre et la gestion d'un programme de cybersécurité en conformité avec la norme ISO/IEC 27032.

2. Objectifs

- Acquérir des connaissances approfondies sur les composantes et les opérations d'un programme de cybersécurité en conformité avec l'ISO/IEC 27032 et le cadre de cybersécurité NIST ;
- Comprendre la corrélation entre l'ISO/IEC 27032, le cadre de cybersécurité NIST et d'autres standards internationaux ;
- Maîtriser les concepts, les approches, les normes, les méthodes et les techniques pour établir, mettre en œuvre et gérer efficacement un programme de cybersécurité au sein d'une organisation ;
- Interpréter les lignes directrices de l'ISO/IEC 27032 dans un contexte spécifique ;
- Acquérir l'expertise nécessaire pour planifier, mettre en œuvre et gérer un programme de cybersécurité tel que spécifié dans l'ISO/IEC 27032 et le cadre de cybersécurité NIST ;
- Conseiller une organisation sur les bonnes pratiques de gestion de la cybersécurité.

3. Public cible

Cette formation s'adresse principalement aux professionnels impliqués dans la cybersécurité, nous pouvons citer parmi eux : experts en sécurité de l'information acteurs, professionnels souhaitant gérer un programme de cybersécurité, responsables du développement d'un programme de cybersécurité, praticiens de la cybersécurité, consultants en cybersécurité.

4. Durée

05 jours

5. Prérequis

Il est recommandé que les participant(e)s disposent d'une connaissance fondamentale de la norme ISO 27032 et de connaissances approfondies sur la cybersécurité.

6. Certification

L'examen -PECB Certified ISO 27032 Lead Cybersecurity Manager- est inclus dans le coût de la formation et est disponible en langue française.

L'examen a une durée de trois (3) heures et couvre les sept domaines suivants :
Domaine 1 : Principes et concepts fondamentaux de la cybersécurité
Domaine 2 : Rôles et responsabilités des parties prenantes
Domaine 3 : Gestion des risques liés à la cybersécurité
Domaine 4 : Mécanismes d'attaque et contrôles en cybersécurité
Domaine 5 : Partage de l'information et coordination
Domaine 6 : Intégrer le programme de cybersécurité dans la continuité des activités
Domaine 7 : Gestion des incidents de cybersécurité et mesure de la performance.

7 Programme

Jour 1 Introduction à la cybersécurité et aux concepts connexes

Jour 2 Politiques de cybersécurité, gestion des risques et mécanisme d'attaque

Jour 3 Mesures de contrôle en cybersécurité, partage et coordination de l'information

Jour 4 Gestion des incidents, suivi et amélioration continue

Jour 5 Préparation à l'examen et examen de certification