ISO 27034, sécurité des applications, Lead Auditor, certification

★★★★★

PL-76 **5 Jours (35 Heures)**

Description

Ce cours intensif de 5 jours permet aux participants de comprendre les principes et les concepts de la sécurité applicative selon ISO 27034 mais aussi de développer l'expertise nécessaire pour préparer et réaliser des audits internes et externes soit pour une organisation soit pour une application.

À qui s'adresse cette formation ?

Pour qui

Auditeurs internes ou externes, gestionnaires de projets, consultants, membres de l'équipe SI d'une organisation, développeurs, directeurs et gestionnaires des applications.

Prérequis

Aucune

Les objectifs de la formation

- Acquérir l'expertise requise pour réaliser un audit interne ISO 27034 qui respecte les exigences de la norme ISO 19011
- Acquérir l'expertise pour réaliser un audit de certification ISO 27034 qui respecte les exigences d'ISO 17021 et 27006
- Acquérir l'expertise requise pour gérer une équipe d'audit en Sécurité
- ApplicativeComprendre la portée, le cycle de vie et les limites de conformité d'une organisation ou d'une application à ISO 27034

Programme de la formation

Introduction aux concepts de la sécurité applicative

- Revue des principes fondamentaux en sécurité de l'information.
- Vision globale de la norme ISO 27034.
- Concepts, principes, définitions, portée, composants, processus et acteurs impliqués en sécurité applicative.
- Concepts implicites intégrés à la norme.
- Avantages et limites de ISO 27034.
- Différences et complémentarité avec les critères communs et le CMMI.
- Le Cadre Normatif de l'Organisation (CNO) et le processus de certification ISO/CEI 27034.
- Présentation détaillée des sections 6 à 8 d'ISO/IEC 27034-1:2011.

Introduction à l'audit de la sécurité applicative

- Concepts d'audit fondamentaux et principes selon ISO 19011.
- La communication durant un audit.
- Procédures d'audit.
- L'audit documentaire.
- Audit sur site et formulation des constats d'audit, documenter les non-conformités.
- Revue de qualité de l'audit.
- Évaluation des plans d'actions correctives.

L'audit de sécurité applicative selon ISO 27034

- Approche basée sur la priorisation des risques de sécurité inacceptables et sur la production de preuves.
- Audit de surveillance ISO/CEI 27034.
- Programme de gestion d'audit interne ISO/CEI 27034.
- Préparation d'un audit de certification ISO 27034.
- Entente sur le périmètre de l'audit de sécurité applicative.
- Détermination des applications dans le périmètre.
- Détermination des éléments de sécurité applicative dans le périmètre pour chaque application.

Audit au niveau de l'organisation

- Entente sur le périmètre de l'audit de SA pour l'organisation.
- Le Cadre Normatif de l'Organisation (CNO).
- La gestion du CNO.
- Les objectifs de sécurité applicative de l'organisation.

Audit au niveau des applications

- Entente sur le périmètre de l'audit de sécurité applicative pour l'application.
- Le cadre normatif de l'application (CNA).
- Le processus de gestion de la sécurité applicative au niveau du CNA.
- Niveau de confiance et CSA.
- ISO 27034 - Révision finale.
- Questions-réponses.

Examen de certification

- Examen Examen de certification ISO 27034 Lead Auditor.