03 20 61 95 06
formation@access-it.fr

FORMATION ISO 27001 ET 27002 - FONDAMENTAUX

2 jours

OBJECTIFS

- Être capable de présenter la norme ISO 27001:2013, les processus de sécurité qui lui sont associés et la démarche de certification
- Savoir présenter la norme ISO 27002 et les mesures de sécurité
- Pouvoir comprendre les contextes d'implémentation des mesures de sécurité et leur intégration dans l'organisation générale de la sécurité
- Apprendre à s'exercer à la sélection et l'approfondissement de mesures de sécurité depuis l'appréciation des risques, les pièges à éviter et l'audit de ces mesures
- Pouvoir disposer d'une vue globale des référentiels existants, des guides d'implémentation ou des bonnes pratiques des mesures de sécurité

PREREQUIS

Culture dans le domaine de la sécurité de l'information

PUBLIC

- Toute personne qui souhaite prendre connaissance des normes ISO 27001 et 27002, améliorer leur maîtrise des mesures de sécurité de l'information et enrichir leur connaissance des référentiels existants pour faciliter leur mise en œuvre
- Opérationnels (techniques ou métiers) et auditeurs souhaitant améliorer leur compréhension des mesures propres à la SSI
- RSSI souhaitant avoir un panorama des mesures, organiser leur plan d'action, ou dynamiser les échanges avec les opérationnels

PROGRAMME

INTRODUCTION AUX SYSTÈMES DE MANAGEMENT

HISTORIQUE DES NORMES

L'ORGANISATION DE LA SÉCURITÉ

PRÉSENTATION DÉTAILLÉE DE LA NORME ISO 27001

L'ORIGINE DES MESURES

La conformité
La gestion des risques
Les ACP ou initiatives internes

INTRODUCTION À LA GESTION DES MESURES DE SÉCURITÉ

Les différents acteurs
Identification des contraintes
Typologies de mesures de sécurité
Plan d'action sécurité
Documentation
Audit des mesures

LA NORME ISO 27002

Présentation et historique
Structure et objectifs
Exemple d'application du modèle PDCA aux mesures
Cas pratique positionnant le stagiaire dans le rôle de : gestionnaire des risques, implémenteur de mesures de sécurité, auditeur

LES RÉFÉRENTIELS DE MESURES DE SÉCURITÉ

Les référentiels sectoriels (HDS, ARJEL, PCI-DSS, SAS-70/ISAE3402/SOC 1-2-3, RGS)
Les autres sources de référentiels et guides de bonnes pratiques : organismes étatiques (Guide d'hygiène de l'ANSSI, NIST, NSA, etc.), les associations et instituts (SANS, OWASP, CIS, Clusif, etc.), les éditeurs

EXAMENS DE CERTIFICATION

Révision des concepts en vue du passage des certifications
Examens blancs
Passage des 2 examens écrits de certification (la certification ISO 27001 est en français tandis que la 27002 est en anglais) qui consiste à répondre à 12 questions en 2 heures
Un score minimum de 70% est exigé pour réussir l'examen

Ce cours est disponible au format :
Présentiel

Ref. ISO 27001

Moyens Pédagogiques et techniques mises en œuvre
Lors des formations en présentiel, nous mettons à disposition tout le matériel de formation nécessaire :
1 PC et 1 support de cours par participant + 1 PC animateur + 1 vidéo projecteur + 1 paperboard.
Les postes sont équipés de l'environnement (logiciel et matériel) recommandé par les éditeurs.
Chaque poste est connecté à internet à notre serveur.

En amont de la formation,
un audit (entretien physique ou téléphonique) préalable nous permet de déterminer et fixer la meilleure approche pédagogique pour atteindre une qualité de formation optimale.

Chaque stagiaire reçoit :
– Le programme de la journée et du module
– Un support de formation
– Un suivi de formation et des échanges entre le formateur et les participants sont proposés

Validation et sanction de la formation
Une attestation mentionnant les objectifs, la nature et la durée de l'action et les résultats de l'évaluation des acquis de la formation sera remise au stagiaire à l'issue de sa formation

Type de formation
Professionnalisante ayant pour objectif le perfectionnement, l'élargissement des compétences