PROGRAMME DE FORMATION
MISE EN CONFORMITÉ ISO27001

Objectifs pédagogiques :

À l'issue de la formation « Introduction à la cybersécurité », vous serez en mesure de :

- Expliquer les composants d'un système de management de la sécurité de l'information (SMSI) conforme à ISO 27001
- Adapter les exigences de la norme ISO27001 au contexte spécifique
- Passage de la certification

Prérequis :

- Maîtrise de l'outil informatique et de la langue française.

Public cible :

- RSSI, Risk Managers, directeurs ou responsables informatiques, ingénieurs ou correspondants Sécurité, chefs de projets, auditeurs internes et externes, futurs "audités".

Modalités pédagogiques :

- Tout au long de la formation, des temps théoriques alternent avec des temps pratiques. Des supports écrits sont transmis au stagiaire en versions numérique et papier. En amont de la formation, un entretien téléphonique est réalisé pour définir les besoins et demandes des stagiaires afin que la formation corresponde au mieux.
- Présentiel : En appui des temps théoriques, un diaporama et un écran mural sont utilisés, tout en laissant place à une forte interactivité entre les stagiaires et les formateurs.
- Distanciel : Une solution à distance permettant la vidéo, le son, le partage d'écran, l'enregistrement des sessions, est utilisée : la formation est ainsi organisée sous la forme de classe virtuelle.

Modalités d'évaluation :

- Un test de fin de formation (QCM, exercices, projet, présentation orale) est réalisé afin de valider les acquis.
- Une attestation de compétences validant les compétences acquises, non acquises et en cours d'acquisition sera remise à chaque stagiaire à l'issue de la formation.
- Chaque stagiaire est invité à participer à un bilan oral " à chaud complété par un questionnaire "à froid" envoyé quelques semaines plus tard, pour connaître l'impact de la formation suivie et d'en mesurer les apports au niveau professionnel.
- Une attestation de présence sera remise au stagiaire à l'issue de la formation.
- Dans le cas des formations à distance, un certificat de réalisation est délivré.

Formateurs :

- Experts dans le milieu de la cyber sécurité.

CONTENU DE LA FORMATION

Introduction

- Rappels. Terminologie ISO 27000 et ISO Guide 73
- Définitions : menace, vulnérabilité, protection
- La notion de risque (conséquence, impact, vraisemblance)
- La classification minimale CID (Confidentialité, Intégrité, Disponibilité)
- La gestion du risque (réduction, maintien, refus, partage)
- Analyse de la sinistralité. Tendances. Enjeux
- Les réglementations de sécurité (métiers, juridiques, …) exemple PCI-DSS, NIST, LPM/NIS. Pour qui ? Pourquoi ?
- L'alignement ISO avec Gouvernance / Protection / Défense / Résilience.

Les normes ISO 2700x

- Historique des normes de sécurité vues par l'ISO
- Les standards BS 7799, leurs apports à l'ISO
- Les normes actuelles (ISO 27001, 27002)
- Les normes complémentaires (ISO 27005, 27004, 27003…)
- La convergence avec les normes qualité 9001 et environnement 14001
- L'apport des qualiticiens dans la sécurité

La norme ISO 27001:2022

- Définition d'un Système de management de Sécurité de l'Information (ISMS)
- Objectifs à atteindre par votre SMSI
- L'approche "amélioration continue" comme principe fondateur, le modèle PDCA (roue de Deming)
- La norme ISO 27001 intégrée à une démarche globale de gouvernance de la SSI
- Détails des phases Plan-Do-Check-Act

- De la spécification du périmètre SMSI au SoA (Statement of Applicability)
- Les recommandations de l'ISO 27001 pour le management des risques.
- De l'importance de l'appréciation des risques. Choix d'une méthode type ISO 27005:2018 / ISO 31000
- L'apport des méthodes publiées (exemple EBIOS) dans leur démarche d'appréciation
- L'adoption de mesures de sécurité techniques et organisationnelles efficientes
- Les audits internes obligatoires du SMSI. Construction d'un programme d'audit
- L'amélioration SMSI. La mise en œuvre d'actions correctives et préventives

Les bonnes pratiques, référentiel ISO 27002:2022

- La structuration du premier niveau : mesures organisationnelles, liées aux personnes, d'ordre physique, technologiques
- Les thèmes et attributs
- Les concepts de cybersécurité
- Les capacités opérationnelles
- Les domaines de sécurité
- La norme ISO 27002:2022 : aperçu des 93 bonnes pratiques
- Les nouvelles bonnes pratiques ISO 27002:2022, les mesures supprimées de la norme ISO 27001:2017
- Exemples d'application du nouveau référentiel à son organisme : les mesures de sécurité clés indispensables

La mise en œuvre de la sécurité dans un projet SMSI

- Des spécifications sécurité à la recette sécurité
- Comment respecter la PSSI et les exigences de sécurité ?
- De l'analyse de risques à la construction de la déclaration d'applicabilité
- Intégration de mesures de sécurité au sein des développements spécifiques
- Les règles à respecter pour l'externalisation
- Assurer un suivi du projet dans sa mise en œuvre puis sa mise en exploitation
- Les rendez-vous "Sécurité" avant la recette
- Intégrer le cycle PDCA dans le cycle de vie du projet
- La recette du projet, comment la réaliser ? Quels types d'audit ?

- Préparer les indicateurs. Indicateurs d'efficacité et de conformité.
- Mettre en place un tableau de bord de gouvernance
- L'apport de la norme 27004 :2016 dans la construction des métriques

La certification ISO de la sécurité du SI : le certificat SMSI

- Intérêt de cette démarche, la recherche du "label"
- Les critères de choix du périmètre
- L'ISO : complément indispensable des cadres réglementaires et standards ?
- Les enjeux business et/ou réglementaires escomptés
- Organismes certificateurs, choix en France et dans le monde
- Démarche d'audit, étapes et charges de travail.
- Normes ISO 17021 et ISO 27006, obligations pour les certificateurs
- Coûts de la certification, ROI

Examen

L'examen est composé d'un questionnaire à choix multiples/questions à trous. Il dure 2h30. Il est valorisé à 100 points. Si au moins 50% des réponses sont correctes l'examen est réussi.