CYBER ESTUAIRE

SENSIBILISATION À LA NORME ISO 27001

PROGRAMME DE FORMATION · 7 HEURES

Introduction · Clauses 4 à 10 · Annexe A · Mise en œuvre · Audit de certification

CYBER ESTUAIRE

PRÉSENTATION

Une journée pour amorcer sereinement votre démarche de certification

Cyber-Estuaire accompagne les entreprises qui n'ont pas encore engagé leur Système de Management de la Sécurité de l'Information (SMSI). Cette formation donne à chaque partie prenante — direction, RSSI, responsables de service — le socle de connaissance et le niveau de responsabilité attendu avant de démarrer le projet.

Pour qui ?

Direction et comité de pilotage du projet, RSSI ou futur pilote du SMSI, responsables de service impliqués dans le périmètre certifié.

Durée & format

7 heures sur une journée, 4 à 12 participants, en intra-entreprise, sur site ou à distance.

Investissement

1 400 € HT, éligible OPCO. Attestation de formation et documentation ISO 27000 remises à chaque participant.

Documentation incluse

Chaque participant repart avec la famille des normes ISO 27000 au format PDF, dont l'ISO 27001:2022 (dernière révision), pour disposer du texte de référence tout au long de son projet.

CYBER ESTUAIRE

PROGRAMME · 7 HEURES

5 modules pour comprendre la norme et lancer le projet

Une progression pensée pour aller de la théorie à l'action, jusqu'aux attendus concrets de l'audit de certification.

1 **Introduction à l'ISO 27001** ~1h

Origine, structure, cycle PDCA, enjeux business et étapes clés d'un parcours de certification.

2 **Les clauses 4 à 10** ~2h

Le système de management : contexte, leadership, planification, support, fonctionnement, évaluation, amélioration.

3 **L'Annexe A** ~1h30

Les 93 mesures de sécurité réparties en 4 thèmes, et la Déclaration d'Applicabilité (SOA).

4 **Mettre en œuvre** ~1h30

De la clause à l'action : politique SSI, traitement des risques, responsabilités de chacun.

5 **Ce qu'attend l'auditeur** ~1h

Déroulement de l'audit de certification, preuves attendues, non-conformités et feuille de route pour lancer le projet SMSI.

CYBER ESTUAIRE

PROGRAMME DÉTAILLÉ

Modules 1 & 2 — Poser les bases

MODULE 1 · ~1H

Introduction à l'ISO 27001

- Origine et structure de la norme ISO/IEC 27001 et de la famille ISO 27000
- La logique d'amélioration continue : le cycle **Plan-Do-Check-Act** (PDCA)
- Les bénéfices business : confiance client, avantage concurrentiel, réduction des risques
- Les grandes étapes d'un parcours de certification : cadrage, mise en œuvre, audit blanc, certification, surveillance

MODULE 2 · ~2H

Les clauses 4 à 10 : le système de management

- **Clause 4** — Contexte de l'organisme : enjeux, parties intéressées, périmètre du SMSI
- **Clause 5** — Leadership : engagement de la direction, politique de sécurité, rôles
- **Clause 6** — Planification : appréciation et traitement des risques, objectifs
- **Clause 7** — Support : ressources, compétences, sensibilisation, documentation
- **Clauses 8-9-10** — Fonctionnement, évaluation des performances, amélioration continue

Atelier pratique : situer son organisation clause par clause.

CYBER ESTUAIRE

PROGRAMME DÉTAILLÉ

Modules 3 & 4 — De la norme à l'action

MODULE 3 · ~1H30

L'Annexe A : les 93 mesures de sécurité

- Structure en 4 thèmes (version 2022) : organisationnel (37), humain (8), physique (14), technologique (34)
- Comment sélectionner ses mesures selon son propre contexte de risque
- La Déclaration d'Applicabilité (SOA) : rôle et contenu attendu
- Zoom sur les mesures phares : contrôle d'accès, gestion des incidents, cryptographie, continuité d'activité

MODULE 4 · ~1H30

Mettre en œuvre : de la clause à l'action

- Traduire les exigences normatives en plan d'action opérationnel
- Rédiger une politique de sécurité de l'information
- Prioriser le traitement des risques identifiés
- Documentation minimale attendue : registre des risques, SOA, procédures clés

Atelier pratique : cartographier qui, dans l'entreprise, porte quelle responsabilité dans le projet (matrice RACI simplifiée).

CYBER ESTUAIRE

PROGRAMME DÉTAILLÉ

Module 5 — Ce qu’attend l’auditeur

MODULE 5 · ~1H

Le déroulement de l’audit de certification

- Les 2 étapes de l'audit : **Stage 1** (revue documentaire) et **Stage 2** (audit sur site)
- La nature des preuves attendues : enregistrements, entretiens, observations terrain
- Non-conformités mineures et majeures : distinction et délais de traitement
- Le cycle de certification : audit initial, surveillance annuelle, renouvellement à 3 ans

Atelier de clôture : feuille de route pour lancer le projet SMSI, remise à chaque participant.

Documentation incluse

Chaque participant repart avec la famille des normes **ISO 27000 au format PDF**, dont l'**ISO 27001:2022** (dernière révision), pour disposer du texte de référence tout au long de son projet de certification.

CYBER ESTUAIRE

POURQUOI CETTE FORMATION ?

Des différenciateurs concrets pour réussir votre projet

Formateur certifié

Formation animée par un consultant certifié ISO 27001 Lead Auditor, expérience terrain en audit et mise en place de SMSI.

Approche pragmatique

Zéro jargon inutile : des ateliers concrets et une feuille de route utilisable dès le lendemain.

Documentation offerte

Famille des normes ISO 27000 fournie en PDF, dont l'ISO 27001:2022, dernière révision.

Éligible OPCO

Organisme de formation déclaré (NDA 11 75 75586 75), prise en charge possible selon votre branche.

Une formation pensée pour engager toute l'entreprise — pas seulement le RSSI — dans la réussite du projet de certification.

CYBER ESTUAIRE

CONTACTEZ-NOUS !

RDV de 30 minutes, et devis sous 48h

https://cal.com/xgougat

contact@cyber-estuaire.fr

cyber-estuaire.fr

+33 (0)6 61 88 84 84

Votre expert Grand Ouest : M. Xavier Gougat

Nantes · Saint-Nazaire

Rennes · Angers