

Séminaire de 3 jour(s)  
Réf : ASE

## Participants

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

## Pré-requis

Connaissances de base de la sécurité informatique.

Prix 2020 : 2690€ HT

## Dates des sessions

### LYON

09 mar. 2020, 12 oct. 2020  
07 déc. 2020

### NANTES

23 mar. 2020

### PARIS

27 jan. 2020, 23 mar. 2020  
25 mai 2020, 06 juil. 2020  
21 sep. 2020, 23 nov. 2020

### TOULOUSE

10 fév. 2020, 15 juin 2020

## Modalités d'évaluation

Les apports théoriques et les panoramas des techniques et outils ne nécessitent pas d'avoir recours à une évaluation des acquis.

## Compétences du formateur

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

## Moyens pédagogiques et techniques

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études

# Implémenter et gérer un projet ISO 27001:2013 préparation aux certifications

*La norme internationale de maîtrise du risque ISO/CEI 27001 lié à la sécurité de l'information décrit, les bonnes pratiques à mettre en place pour qu'une organisation puisse maîtriser efficacement les risques liés à l'information. Ce cours présente les normes ISO de la sécurité du Système d'Information puis les éléments pour mettre en place un système de management (SMSI) du risque de la sécurité de l'information.*

## OBJECTIFS PEDAGOGIQUES

Expliquer les composants d'un système de management de la sécurité de l'information (SMSI) conforme à ISO 27001

Expliquer le contenu et la corrélation entre ISO 27001 et 27002 ainsi qu'avec d'autres normes et cadres réglementaires

Adapter les exigences de la norme ISO 27001 au contexte spécifique d'un organisme

Interpréter les exigences d'ISO 27001 dans le cadre de l'audit d'un SMSI

Aligner les différentes approches de la gouvernance SSI (ISO, LPM, NIS, ...)

### 1) Introduction

### 2) Les normes ISO 2700x

### 3) La norme ISO 27001:2013

### 4) Les bonnes pratiques, référentiel ISO 27002:2013

### 5) La mise en œuvre de la sécurité dans un projet SMSI

### 6) Les audits de sécurité ISO 19011:2018

### 7) La certification ISO de la sécurité du SI

## Travaux pratiques

Préparation aux certificats ISO 27001 Lead Implementer et Lead Auditor.

## 1) 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 métiers PCI-DSS, COBIT. Pour qui ? Pourquoi ? Interaction avec l'ISO.
- Vers la gouvernance IT, les liens avec ITIL® et l'ISO 20000.
- L'alignement ISO – NIS/LPM : vers une convergence ?

## 2) Les normes ISO 2700x

- Historique des normes de sécurité vues par l'ISO.
- Les standards BS 7799, leurs apports à l'ISO.
- Les normes fondatrices (ISO 27001, 27002).
- Les normes indispensables (ISO 27005, 27004, 27003, etc).
- La convergence avec les autres normes « Système de Management ».

## 3) La norme ISO 27001:2013

- Définition d'un Système de Gestion de la Sécurité des Systèmes (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.
- L'apport des méthodes publiées (exemple EBIOS RM) dans leur démarche d'appréciation.
- L'adoption de mesures de sécurité techniques et organisationnelles efficaces.
- Les audits internes obligatoires du SMSI. Construction d'un programme d'audit.
- L'amélioration SMSI. La mise en œuvre d'actions correctives et préventives.
- L'annexe A comme support référentiel - lien avec la norme 27002.

## 4) Les bonnes pratiques, référentiel ISO 27002:2013

- Objectifs de sécurité : Disponibilité, Intégrité et Confidentialité.
- Structuration en domaine/chapitres (niveau 1), objectifs de contrôles (niveau 2) et contrôles (niveau 3).
- Les nouvelles bonnes pratiques ISO 27002:2013, les mesures supprimées de la norme ISO 27001:2005. Les modifications.
- La norme ISO 27002:2013 : les 14 domaines et 114 bonnes pratiques.
- Exemples d'application du référentiel à son entreprise : les mesures de sécurité clés indispensables.

de cas ou présentation de cas réels pour les séminaires de formation.

- A l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.

- Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

- Les mesures de la réduction des risques sur les actifs supports type personnes, bien, informatique.
- Les mesures indispensables au partage via le domaine 15.

## 5) 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 du client/MOA ?
- 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 ? Test d'intrusion et/ou audit technique ?
- Préparer les indicateurs. L'amélioration continue.
- Mettre en place un tableau de bord. Exemples.
- L'apport de la norme 27004 :2016 dans la construction des métriques de conformité et efficacité.
- La gestion des vulnérabilités dans un SMSI : scans réguliers, Patch Management...

## 6) Les audits de sécurité ISO 19011:2018

- Processus continu et complet. Étapes, priorités.
- La construction du programme d'audits internes.
- Les catégories d'audits, organisationnels, techniques, etc.
- L'audit interne, externe, tierce partie.
- Le déroulement type ISO de l'audit, les étapes clés.
- Les objectifs d'audit, la qualité d'un audit.
- La démarche d'amélioration pour l'audit.
- Les qualités des auditeurs, leur évaluation.
- L'audit organisationnel : démarche, méthodes.

## 7) La certification ISO de la sécurité du SI

- Intérêt de cette démarche, la recherche du "label".
- Les critères de choix du périmètre. Domaine d'application. Implication des parties intéressées.
- 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.