Devenir Responsable de la Sécurité des Systèmes d'Information (RSSI / CISO)

Référence	Durée	Dates Paris	Coût
SI RSSI	6 jours : 2 *3 jours (42 heures)	Voir calendrier Inter	Nous consulter

Avis de l'expert

La protection de l'information et la sécurité des systèmes d'information revêt aujourd'hui une telle importance que les responsables de la sécurité des systèmes d'information doivent être de plus en plus impliqués dans les processus de gouvernance de l'entreprise ou de l'organisme. La mission du RSSI est essentielle puisqu'il a la charge des actions relatives à la protection de l'information et la sécurité des systèmes, des réseaux, des applications et des données de l'entreprise. Cette formation, illustrée de nombreux cas concrets, fournira aux participants toutes les bonnes pratiques clés pour maîtriser les dimensions de ce métier.

Objectifs de la formation

- Identification de toutes les missions du métier de responsable sécurité, son rôle et ses responsabilités
- Démarche complète pour construire une politique de sécurité et gérer les risques du SI
- Panorama des mesures techniques de protection des systèmes d'information
- Méthodes pour assurer la mise en œuvre et le suivi de la sécurité
- Bonnes pratiques pour construire son plan d'action et définir ses indicateurs

Itinéraire pédagogique

Première partie (3 jours) :

1. **Introduction : Quels sont les enjeux de la SSI ?**
   - Quelques définitions, périmètres et terminologies de base
   - Les enjeux de la sécurité de l'information
   - La nature des menaces et des risques

2. **Les missions du RSSI**
   - Conseil Direction Générale obligations légales et risques SSI
   - Formalisation d'une stratégie et définition d'un plan d'actions
   - Définition d'un référentiel SSI
   - Participation à la mise en en place de la gouvernance
   - Conseil et assistance maitrise d'ouvrage pour la gestion des risques
   - Conseil, assistance et contrôle maitrise d'œuvre pour le traitement des risques
   - Formation sensibilisation
   - La veille
   - Audits, contrôles de conformité et d'efficacité

3. **Les obligations légales et les exigences SSI**
   - Responsabilités civile délictuelle et contractuelle
   - Les obligations légales
   - PPST : Protection des informations relatives au potentiel technique de la nation
   - Respect de la vie privée / Secret des correspondances
   - GDPR
   - Loi pour une république numérique
   - SOX : Sarbanes Oaxley
   - LSF : La Loi de Sécurité Financière
   - LCEN : Loi Confiance dans l'Economie Numérique
   - LSQ : Loi Sécurité Quotidienne / Loi Godfrain
   - CPI : Code de la Propriété Intellectuelle
   - La directive « Network and Information Security»
   - LMP : Loi de Programmation Militaire

4. **Identification des autorités compétentes et référentiels**

- ANSSI, PSSI x, RGS,
- Agence Française de la santé numérique
- PCI DSS

5. **Les contrats**

6. **Gouvernance de la SSI :**
   - Niveaux de maturité SSI et types d'organisation
   - Le comité de pilotage, arbitrage, suivi et homologation
   - Voie hiérarchique et voie fonctionnelle
   - Les articulations avec les autres filières, (hiérarchique, sécurité des installations, gestion de crises, …)
   - La notification d'incidents, la gestion d'alerte

7. **Formalisation d'une stratégie SSI**
   - Adjonction d'outils et bonnes pratiques
   - Orientée enjeux
   - Orientée SMSI
   - Formalisation d'une feuille de route
     - Les étapes

8. **La gestion des risques**
   - La norme ISO 31000
   - La norme ISO 27005
     - L'assistance à la maitrise d'ouvrage pour l'évaluation des besoins et évènements redoutés
     - L'assistance à la maitrise d'œuvre pour le traitement des risques
     - Conseil pour la validation ou l'homologation
   - Etudes de cas
   - La norme ISO 27002
   - La norme ISO 27001

9. **La définition d'un référentiel SSI**
   - Lettre d'engagement direction
   - Lettre de nomination RSSI
   - Politique générale de protection de l'information
   - Comment construire la politique sécurité système d'information
   - Chartes
   - Guides et procédures

10. **Mise en œuvre d'une méthode d'intégration SSI dans les projets**
    - EBIOS
    - Adaptée

Deuxième partie (3 jours) :

11. **L'état de l'art des solutions techniques de sécurité système d'information**
    - La sécurité des accès
      - Filtrages
      - Authentifications
      - Habilitations
      - Détections
      - Journalisations
    - La sécurité des échanges
      - Chiffrements symétriques et asymétriques
      - Infrastructure à gestion de clés publiques
      - Les déclinaisons
    - La sécurité des serveurs
      - Durcissement
      - Hébergement
    - La sécurité des postes de travail sédentaires et mobiles
    - La sécurité des applications

12. **Les architectures SSI**
    - Périphériques

- En profondeur

13. Introduction aux plans de continuité des activités et plans de secours
- Fondamentaux de la continuité des activités
- Le modèle du BCI et de la norme ISO 22301
- Les différents plans : PCA, PCO, PSI, PGC, PCOM...
- Les phases d'un projet de PCA

14. La prise en compte du facteur humain
- La sensibilisation / Formation / communication

15. La veille juridique et technique SSI

16. Contrôle et audit
- Définition des indicateurs de contrôle
- Les tests intrusifs
- Formalisation et mise à jour des tableaux de bord

17. Conseils généraux pour réussir dans son métier de RSSI
- Les freins et les difficultés rencontrés par les RSSI (retours d'expérience)
- La bonne appropriation et la bonne communication du rôle du RSSI
- Les erreurs à ne pas commettre, les conseils d'accompagnement au changement

Déroulement du stage

L'approche méthodologique participative permet des échanges entre les participants et le formateur sur des retours d'expériences concrets : le formateur accompagne des RSSI depuis plusieurs années dans l'accomplissement de leurs missions.

Le support de formation est utilisé pour présenter les éléments théoriques et les applications pratiques dans le domaine de la sécurité des systèmes d'information. Il est adapté au contexte actuel et aux obligations réglementaires en vigueur.

Des documents annexes illustrent les cas concrets abordés durant la formation.

Public concerné

- Responsables métiers ou informatiques souhaitant évoluer vers le métier de RSSI
- RSSI opérationnels souhaitant appréhender les nouvelles missions du RSSI

Contrôle des acquis

Cette formation ne fait pas l'objet d'une évaluation des acquis. En fin de stage, une attestation de formation est remise au participant.

Pré-requis

Bonne culture générale sur les infrastructures IT.

Inscription

Renseignements et inscriptions au +33 (0)3 87 62 06 00 ou contact@ageris-group.com

Votre inscription donne lieu à l'établissement d'une convention de formation professionnelle sur demande. Chaque participant reçoit une convocation lui donnant toutes les indications nécessaires sur l'organisation matérielle de sa formation 2 semaines avant le début de sa formation.

Notre numéro d'activité déclarée en tant qu'organisme de formation est le 4157 02486 57 du 16/05/2006.

DataDock Nr 0034584