RSSI - Responsable Sécurité des Systèmes d'information

Durée: 5 Jours **Réf de cours: GKRSSI** **Version: 1**

Résumé:

Dans un contexte où les cyberattaques se multiplient et où la résilience numérique devient une priorité stratégique, cette formation de 5 jours permet aux participants de maîtriser les fondamentaux du rôle de Responsable de la Sécurité des Systèmes d'Information (RSSI) ainsi que les étapes de mise en œuvre d'un Système de Management de la Sécurité de l'Information (SMSI) conforme à la norme ISO/IEC 27001.

La formation s'appuie sur une alternance d'apports théoriques, de cas pratiques et de labs techniques pour une montée en compétence progressive et concrète. Elle s'adresse autant aux profils en prise de poste qu'aux collaborateurs en reconversion vers les métiers de la cybersécurité.
Msie à jour : 16.12.2025

Public visé:

Toute personne amenée à exercer la fonction de responsable sécurité des systems d'information : RSSI, futurs RSSI, RSSI adjoint, …

Objectifs pédagogiques:

- A l'issue de la formation, le stagiaire sera capable de :
- Comprendre les enjeux de la sécurité des services informatique dans une organisation
- Connaître les techniques de base de la fonction RSSI
- Maîtriser la norme ISO 27001 et mettre en œuvre un SMSI dans son organisation
- Connaître la politique de sécurité et auditer la sécurité et les indicateurs
- Connaître les règlementations et aspects juridiques de la sécurité des systèmes informatiques
- Savoir réagir face à un incident

Pré-requis:

- Avoir une expérience au sein d'une direction informatique en tant qu'informaticien.
- Avoir des notions de base en sécurité appliquées aux systèmes d'information et une bonne maîtrise des systèmes et des infrastructures

Test et certification

- Aucune

Contenu:

Journée 1

Démarrage de la formation

Présentation des enjeux, tour de table des participants, identification des attentes, présentation du déroulé pédagogique et des modalités d'évaluation.

Module 1 Introduction à la sécurité de l'information

- Concepts et définitions en relation avec la sécurité de l'information
- Différence entre sécurité informatique et sécurité de l'information
- Management de la sécurité de l'information
- Problèmes dus à la mauvaise gestion de la sécurité
- Acteurs intervenant dans la sécurité de l'information
- Cadres normatifs et règlementaires

ACTIVITÉ : LAB 1 : Quizz

Module 2 RSSI dans une organisation

- Rôle du RSSI dans une organisation
- Relation RSSI et direction
- Relation RSSI et autres collaborateurs
- Mission au quotidien du RSSI

ACTIVITÉ : LAB 2 : Quizz

Module 3 Présentation de la famille ISO 27000

- Historique de la norme ISO 27001
- Rôle de chaque norme / guide 2700X
- Complémentarité des normes ISO 2700X
- Processus de certification et de conformité.

ACTIVITÉ : LAB 3 : Quizz

Module 4 Présentation de la norme ISO 27001

- Architecture de la norme ISO 27001.
- Revues des chapitres de la norme ISO 27001

ACTIVITÉ : LAB 4 : Quizz

Journée 2

ACTIVITÉ : LAB 5 : Analyse d'un cas d'une organisation pour analyser son contexte et identification des enjeux

Module 6 Leadership

- Engagement de la direction et relation avec le RSSI
- Politique de sécurité de l'information
- Rôle du middle Management

ACTIVITÉ : LAB 6 : Présentation d'une panoplie de politiques d'organisation pour comprendre le format d'une politique

Module 7 Analyse des Risques

- Identification des actifs
- Relation entre actifs et enjeux
- Identification des menaces
- Identification des scénarios des risques
- Apports des méthodologies pour faciliter l'analyse des risques

ACTIVITÉ : LAB 7 : Elaboration des scénarios de risques pour des cas de figure

Module 8 Traitement des risques et déclaration d'applicabilité

- Options de traitement des risques
- Exemples de mesures de traitements de risques
- Annexe A comme sources de mesures de traitement des risques
- Déclaration d'applicabilité

ACTIVITÉ : LAB 8 : Présentation de cas de risques et mise en pratique pour la conception de mesure de traitements des risques

Journée 3

Module 9 RH et Responsables en termes de sécurité de l'information

- Processus de recrutement conforme à la norme ISO 27001
- Clauses de confidentialité dans les contrats
- Principaux responsables en termes de sécurité de l'information et fiches poste associés
- Processus de départ conforme à la norme ISO 27001

ACTIVITÉ : LAB 9 : Quizz

Module 12 Mécanismes d'amélioration continue de la norme ISO 27001

- Indicateur de performances
- Audit
- Revue de la direction
- Gestion des non-conformités et actions correctives

ACTIVITÉ : LAB 12 : Exercices portant sur la relève de situation des non-conformités de cas de figure

Journée 4

Module 13 Simulation de mise en œuvre (Objectifs : O3, O4)

- Étude de cas : mise en place de processus de sécurité
- Rédaction collaborative : politique, procédure, plan de traitement

ACTIVITÉ : LAB 13 : Développement de livrables de sécurité en équipe

Module 14 Atelier de synthèse / retour d'expérience

- Discussion ouverte sur les choix réalisés
- Préparation à la restitution
- Journée 5 Matin
- Module 15 Restitution des travaux des stagiaires (O4)
- Chaque stagiaire présente ses documents
- Discussion

Journée 5

Module 15 Restitution des travaux des stagiaires

- Chaque stagiaire présente ses documents
- Discussion

Module 16 Loi et règlements en termes de sécurité de l'information

- La loi Godfrain
- Loi de programmation militaire
- La Loi Informatique et Liberté
- Le Règlement Général de la protection des données personnelle

ACTIVITÉ : LAB 14 : Quizz et Mise en situation

Module 17 Processus et gestion de réponse

Module 5 Analyse du contexte et identification des enjeux

- Identification des parties intéressées pertinentes pour la sécurité de l'information
- Identification des besoins des parties intéressées
- Identification des exigences légales

Module 10 Annexe A ISO 27001

- Mesures Organisationnels
- Mesures de sécurité applicables aux personnes
- Mesures de sécurité physique
- Mesures de sécurité technologiques

ACTIVITÉ : LAB 10 : Exercices portant sur la mise en relation entre les mesures de l'Annexe A et les risques.

Module 11 Démarche mise en place SMSI

- Présentation du Modèle PDCA
- Analyse du contexte et des besoins
- Planification et structuration du SMSI
- Mise en œuvre des contrôles
- Surveillance et amélioration continue

ACTIVITÉ : LAB 11 : Quizz

aux incidents

- Terminologie
- Catégorisation des événements et des incidents de sécurité
- Normes relatives à la gestion et aux réponses aux incidents
- Les CERT (computer and emergency response team)
- Phases de prise en charge d'un incident
- Responsabilité dans la gestion des incidents
- Le SOC, SOAR et SIEM
- Tableau de bord des incidents
- Présentation des outils CTI (Cyber Threat Intelligence)

ACTIVITÉ : LAB 15 : Quizz et Mise en situation d'incidents de sécurité

- Clôture de la formation

Méthodes pédagogiques :

Compétences du formateur
Nos formateurs justifient d'au moins 3 ans d'expérience en tant que RSSI ou consultant cybersécurité. Leur double expertise leur permet d'animer des formations stratégiques, combinant pilotage SSI et transmission pédagogique auprès de futurs responsables sécurité.
Répartition Théorie / Pratique
- 40 % Théorie : (Concepts fondamentaux, méthodologies de gestion de la sécurité de l'information, référentiels normatifs ISO 27001 et ISO 27005, cadre légal et réglementaire, stratégie de gouvernance et indicateurs SSI)
- 60 % Pratique : (Labs interactifs, quiz de validation, analyse de scénarios de risques, rédaction de politiques de sécurité, cartographie des actifs, simulation d'incidents, mise en œuvre d'un SMSI, restitution de livrables en groupe)
Ressources & Outils fournis
- Modèles de documents professionnels
- Kits de travaux pratiques (LABS) :
- Outils de simulation et d'évaluation :
- Environnement technique requis : machine virtuelle (VirtualBox ou VMware), accès administrateur, connexion internet stable, Microsoft Office installé.
Méthodes pédagogiques
- Animation participative via des outils collaboratifs, partages d'écran, analyses d'études de cas, exercices collaboratifs et activités de groupe simulant des contextes réels.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement