

RSSI (Responsable de la Sécurité des SI) – Rôles et attentes organisationnelles

5 jours (35 heures)

Perfectionnement

Présentiel ou classe à distance

à partir de

3 675 € HT par personne (TVA en vigueur) Repas inclus en présentiel

Contenu mis à jour le 25/09/2026. Document téléchargé le 07/10/2026.

Objectifs

A l'issue de cette formation, vous serez capable de :

- Mettre en place les bases d'une bonne gouvernance de la sécurité des systèmes d'information
- Reconnaître les techniques de base indispensables à la fonction de RSSI
- Expliquer et mettre en oeuvre un SMSI en vous appuyant sur la norme ISO 27001
- Exploiter l'état du marché de la sécurité informatique
- Identifier les méthodes d'appréciation des risques ainsi que les enjeux de la SSI au sein des organisations
- Mettre en pratique les stratégies de prise de fonction et des retours d'expérience de RSSI
- Identifier et évaluer les principaux risques juridiques pesant sur un système d'information
- Réduire concrètement les non-conformités juridiques affectant un système d'information.

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

Ingénieurs système, ingénieurs en sécurité, administrateurs système, chefs de projets en sécurité, MOE (maîtres d'oeuvre) et/ou MOA (maîtres d'ouvrage).

Prérequis

Avoir des connaissances de base sur la sécurité des systèmes d'information et une bonne maîtrise des systèmes et des infrastructures.

Programme

1 Pendant votre formation

RSSI (Responsable de la Sécurité des SI) – Rôles et attentes organisationnelles

Jour 1 – Fondamentaux et cadre de la fonction RSSI

Introduction

- Définition de la Sécurité du Système d'Information (SSI)
- Critères CIDT, états de la donnée, périmètre de la SSI
- Enjeux stratégiques (économique, juridique, réputationnel, opérationnel)
- Référence documentaire (normes, réglementations, guides ANSSI)
- Paysage des menaces actuelles (ransomware, supply chain, phishing)

Exemple de travaux pratiques (à titre indicatif)

- *Présentation de l'étude de cas fil rouge (documents fournis pour les mises en oeuvre des recommandations)*

Rôles et responsabilités du RSSI

- Elaboration de la politique de sécurité (PSSI, structure type, livrables)
- Gestion des risques (processus, options de traitement)
- Sensibilisation et formation (programme par public, indicateurs)
- Surveillance et audit (types, SIEM, SOC, veille CVE)
- Gestion des incidents (ISO 27035, classification P1-P4)
- Conformité et réglementation (RGPD, NIS2, DORA, LPM)
- Sécurité physique et logique (IAM, MFA, EDR, segmentation)
- Gestion des accès (moindre privilège, cycle de vie)
- Veille technologique (sources, organisation de la veille)
- Relations DSI – RSSI – DSSI – Référents SSI (organigramme, rattachement)
- Coordination avec les autres départements (matrice d'interaction)

Exemple de travaux pratiques (à titre indicatif)

- *Présentation et analyse de la PSSI de l'étude de cas*

Normes et certifications liées

- Référentiels de sécurité (normes, frameworks, réglementations)
- Présentation des normes ISO (famille ISO 27000, structure ISO 27001:2022)
- Système de management dans le cadre des normes ISO270xx (PDCA, Annexe A – 93 mesures)
- Présentation du NIST CSF 2.0 (6 fonctions dont Govern) et de la directive NIS2 (entités essentielles / importantes, article 21, sanctions)
- ISO 22301 (continuité d'activité, concepts BIA / RTO / RPO / MTPD)
- Cyber Resilience Act – exigences produits connectés
- Cyber insurance – exigences assureurs et levier d'investissement
- Certifications personnelles : comparatif CISSP – CISM
- Certification CISSP (8 domaines CBK)
- Certification CISM (4 domaines)

Exemple de travaux pratiques (à titre indicatif)

- *Présentation des documents ISO27001, ISO27005 et NIST*

Organisation générale du SMSI

- Définition du domaine d'application (dimensions, périmètre progressif)
- Politique de sécurité du système d'information (PSSI)
- Analyse et gestion des risques (EBIOS RM, OCTAVE)
- Rôles et responsabilités (matrice RACI)
- Objectifs de sécurité de l'information (SLA, SMART)
- Contrôles et mesures de sécurité (Document d'Applicabilité)
- Gestion des incidents de sécurité
- Sensibilisation et formation
- Amélioration continue
- Conformité et audits
- Gestion documentaire

Exemple de travaux pratiques (à titre indicatif)

- *Présentation de la cartographie applicative, de la matrice de flux et du document d'applicabilité*

Jour 2 – Catégorisation des actifs, supervision, amélioration continue

Catégorisation et sécurisation des actifs

- CIDT et protection de la donnée (échelles, évaluation par actif)
- Inventaire des actifs (structure du registre, outils CMDB)
- Classification de l'information (4 niveaux, règles de manipulation)
- Etiquetage et traitement de l'information (métadonnées, automatisation)
- Protection des actifs (mesures par niveau, DLP endpoint / réseau / cloud)
- Gestion des actifs mobiles et distants (télétravail, BYOD, MDM, Zero Trust)
- Contrôle d'accès aux actifs (RBAC, ABAC, matrice d'habilitation)
- Surveillance et revue des actifs (fréquence, indicateurs)

- Formation et sensibilisation
- Documentation et audit

Exemples de travaux pratiques (à titre indicatif)

- Présentation des matrices de criticité et de sensibilité des actifs
- Présentation des métadonnées du référentiel classifié

Supervision de la sécurité des actifs

- Inventaire et classification des actifs (outils de découverte)
- Propriété et responsabilité des actifs (propriétaire / dépositaire / utilisateur)
- Contrôles d'accès (IAM, revue des accès)
- Protection des actifs (défense en profondeur – 5 couches)
- Document d'applicabilité (ISO27001) – 93 mesures détaillées
- Surveillance et détection des incidents (SIEM, EDR, KPI)
- Gestion du cycle de vie des actifs (mise au rebut sécurisée)
- Evaluation et audit des actifs (scans, pentests)
- Sensibilisation et formation

Exemples de travaux pratiques (à titre indicatif)

- Présentation d'un extrait de Runbook
- Présentation d'un rapport d'incident

Notion de l'amélioration continue

- Présentation du cycle PDCA (Plan-Do-Check-Act)
- Révisions de direction (entrées / sorties, fréquence)
- Rôle de l'audit interne (programme annuel, processus)
- Gestion des non-conformités et actions correctives (fiche NC, 5 Pourquoi)
- Surveillance et mesure (indicateurs, niveaux de reporting)

Exemple de travaux pratiques (à titre indicatif)

- QCM sur l'amélioration continue (PDCA)

Notion du processus qualité (SMI)

- Politique de qualité (convergence qualité / sécurité, ISO 9001 / 27001)
- Objectifs qualité (méthode SMART)
- Engagement de la direction (chapitre 5.1 ISO 27001)
- Documentation (documents obligatoires, maîtrise documentaire)
- Formation et sensibilisation
- Gestion des changements (standard, normal, urgent, CAB)
- Evaluation des fournisseurs et partenaires (grille de notation)

Exemple de travaux pratiques (à titre indicatif)

- QCM sur le processus qualité

Jour 3 – Organisation, compétences relationnelles, juridique, audit

Aspects organisationnels de la sécurité

- Gouvernance de la sécurité de l'information (3 niveaux)
- Implication du sponsor (rôle, profils typiques)
- Organisation interne (rattachement DSI vs DG, NIS2)
- Rôles et responsabilités (matrice RACI détaillée)
- Gestion des risques (processus 5 étapes ISO 27005)
- Présentation du plan de continuité et gestion des incidents (PCA / PRA, RTO / RPO)
- Introduction à la conformité et à l'audit
- Liaison avec les ressources humaines (cycle de vie collaborateur)
- Communication et documentation (documents fondamentaux)

Exemples de travaux pratiques (à titre indicatif)

- *Présentation d'une matrice de rôles (RACI)*
- *Présentation du RBAC*
- *Présentation d'un extrait de PCA / PRA*

Compétences relationnelles du RSSI

- Communication efficace (adapter son discours par audience)
- Leadership (influencer sans autorité hiérarchique)
- Gestion du sponsor (scénarios : budget, DSI réticent)
- Collaboration et travail d'équipe
- Négociation et gestion des conflits (méthode Harvard)
- Empathie et écoute active (5 techniques)
- Sensibilisation et formation (programme, budget)
- Adaptabilité et gestion du changement (modèle ADKAR)
- Board-level reporting – KPI stratégiques et reporting CODIR

Exemple de travaux pratiques (à titre indicatif)

- *Présentation d'une fiche de poste RSSI*

Sécurisation des processus entre fournisseurs et intervenants

- Politique de sélection des fournisseurs (processus achats sécurisé)
- Politique de gestion de la sous-traitance (supply chain, NIS2 art. 21)
- Contrats et accords de service (SLA) – 7 clauses essentielles
- Gestion des accès (6 principes, bastion d'administration)
- Conformité et audits
- Gestion des incidents
- Formation et sensibilisation
- Gestion de la relation fournisseur (revue annuelle)
- Fin de contrat et retrait des accès (processus 5 étapes)

- Cyber ratings et scores de sécurité (SecurityScorecard, BitSight)
- TPRM – Third-Party Risk Management (processus et outils)

Exemple de travaux pratiques (à titre indicatif)

- Présentation d'un questionnaire fournisseur

Aspects juridiques de la SSI

- Conformité légale et réglementaire (panorama EU et France)
- Protection des données personnelles (RGPD) – articles 5, 25, 32, 33, 34, 35
- Articulation DPO / RSSI
- Obligations contractuelles (NDA, clauses sécurité, assurance cyber)
- Propriété intellectuelle (brevets, logiciels, BDD, marques)
- Gestion des incidents de sécurité (ISO27035 – ISO22301)
- Audit et revue de la conformité
- Formation et sensibilisation juridique (par profil, obligation NIS2 direction)
- Gestion des risques juridiques (cartographie)
- AI Act – classification des systèmes IA par risque, obligations du RSSI

Exemple de travaux pratiques (à titre indicatif)

- Démonstration du lien entre les normes et règlements de la PSSI

Audit et conformité des actifs

- Politiques et procédures d'audit (objectifs, principes fondamentaux)
- Planification et préparation des audits (programme triennal, budget)
- Réalisation des audits (phases, types de preuves, constats ISO 19011)
- Analyse des résultats d'audit (fiche NC, cause racine)
- Actions correctives et préventives (méthodologie 5 étapes)
- Surveillance continue et présentation du processus de revue de conformité
- Audit externe et certification (cycle ISO 27001, erreurs classiques)
- Formation et sensibilisation

Exemple de travaux pratiques (à titre indicatif)

- Présentation d'un rapport d'audit ISO27001

Jour 4 – Gestion des risques, continuité d'activité, conduite de projet

Méthode de gestion des risques (EBIOS Risk Manager)

- Différences entre ISO27005 et EBIOS RM (comparatif détaillé)
- Cadre et préparation (équipe, outils, bases de connaissances ANSSI)
- Etape 1 : Analyse du contexte (valeurs métier, biens supports, socle de sécurité)
- Etape 2 : Identification des risques (sources de risque SR, objectifs visés OV, couples SR / OV)
- Etape 3 : Evaluation des risques (écosystème, scénarios stratégiques, chemins d'attaque)
- Etape 4 : Traitement des risques (scénarios opérationnels, modes opératoires MITRE ATT&CK, matrice de risques)

- Etape 5 : Surveillance et revue des risques (risques résiduels, acceptation)
- Documentation et communication (rapport, présentation CODIR)
- MITRE ATT&CK – utilisation pratique pour le RSSI (navigation, cas d'usage SOC)

Exemples de travaux pratiques (à titre indicatif)

- *Présentation des SR-OV en relation avec l'étude de cas (6 SR, 6 OV, 3 scénarios)*
- *Présentation du rapport de traitement des risques (20 mesures, budget, risques résiduels)*

Cycle du SMCA (ISO 22301)

- Contexte de l'organisation (structure HLS)
- Politique et gouvernance
- Analyse de l'impact sur les activités (BIA) – démarche, résultats
- Evaluation des risques
- Stratégies de continuité (hot, warm, cold, dégradé)
- Plans de continuité et procédures (structure PCA, processus d'activation)
- Formation et sensibilisation
- Tests et exercices (PCA / PRA) – 5 types d'exercices
- Méthodologie structurée des exercices tabletop (scénarios, injects, débriefing)
- Surveillance et revue (KPI, déclencheurs de mise à jour)
- Amélioration continue

Exemple de travaux pratiques (à titre indicatif)

- *Présentation d'un PCA / PRA (BIA, stratégies, procédures, fiches réflexe)*

Conduite de projet SMSI

- Initiation du projet dans le contexte de la PSSI (motivations, maturité, Go / NoGo)
- Planification du projet (macro-planning 15 mois, budget 157 K EUR)
- Mise en oeuvre du projet (quick wins vs long terme, gouvernance)
- Surveillance et contrôle du projet (tableau de bord, résistances au changement)
- Clôture du projet et amélioration continue (certification, passage en mode RUN)

Exemple de travaux pratiques (à titre indicatif)

- *QCM sur la conduite de projet*

Jour 5 – Gestion de crises, aspects techniques, développement sécurisé

Gestion de crises (ISO 27035)

- Présentation du processus de préparation et planification (politique, classification, cellule de crise)
- Détection et alerte (sources de détection, qualification, scénario ransomware)
- Réponse et gestion de la crise (confinement, éradication, arbre de décision rançon)
- Coordination et collaboration (notifications légales ANSSI / CNIL, plan de communication)
- Documentation et suivi (main courante, forensics, chaîne de custody)
- Récupération et reprise (plan de reprise 4 phases)

- Amélioration continue (post-mortem, plan d'actions correctives)

Exemples de travaux pratiques (à titre indicatif)

- Présentation d'un formulaire de communication de crise
- Présentation du rapport d'incident complet

Aspects techniques de la sécurité

- Contrôles d'accès (IAM, 3 facteurs, MFA, PAM, gestion des identités)
- Zero Trust – modèle de maturité (principes, 6 piliers, feuille de route progressive)
- Présentation des concepts de sécurisation des réseaux (zones, NGFW, WAF, IDS / IPS, NAC, VPN vs ZTNA)
- Notion de cryptographie (services, symétrique / asymétrique, PKI, certificats)
- Sécurité des applications (OWASP Top 10, questions du RSSI)
- Gestion des correctifs (processus 6 étapes, délais par CVSS)
- Gestion des vulnérabilités (CVSS, CVE, EPSS, programme complet)
- Sécurité des terminaux (pile EDR / DLP / MDM, hardening)
- Surveillance et détection (SIEM, SOC L1-L3, CTI, SOC externalisé)
- Cloud security posture – CSPM, CWPP, CNAPP (convergence, outils, responsabilité partagée)
- Deepfakes et IA offensive – impact opérationnel pour le RSSI (fraude vocale, phishing IA, contre-mesures)
- Planification de la continuité des activités (référence transverse Jour 4)

Exemples de travaux pratiques (à titre indicatif)

- Création de paires de clés publiques / privées et échange de messages entre les participants
- Exercice de simulation de crise

Sécurisation du développement logiciel

- Intégration de la sécurité dans le cycle de vie du développement logiciel (SDLC)
- Conception sécurisée (threat modeling STRIDE, 10 principes)
- Développement sécurisé (standards OWASP, gestion des secrets)
- Présentation du processus de tests de sécurité (SAST, DAST, IAST, SCA)
- Présentation de la gestion des vulnérabilités (SBOM, responsable disclosure)
- Déploiement sécurisé (checklist, PV de recette sécurité)
- DevSecOps – pipeline CI / CD sécurisé (quality gates automatisés)
- Présentation de la surveillance et de réponse aux incidents (logging sécurisé)
- Documentation et conformité
- Maturité DevSecOps – où en est votre organisation (grille de maturité en 4 niveaux)

Exemple de travaux pratiques (à titre indicatif)

- Présentation d'un cahier de recette sécurité

Conclusion et mise en perspective

- Synthèse des 5 jours (compétences acquises, livrables)
- Les 100 premiers jours du RSSI (plan d'action prise de poste)

- Roadmap sécurité sur 3 ans
- Evolutions réglementaires à anticiper (NIS2, DORA, CRA, AI Act, EUCS)
- Evolution des menaces (RaaS, supply chain, IA offensive, attaques sur l'identité)
- Tendances technologiques (Zero Trust, SASE, XDR, SOAR, IA défensive)
- Evolution du rôle du CISO (burnout, metrics-driven security, board communication)
- Certifications recommandées (parcours de développement)
- Ressources essentielles du RSSI

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

[Nous contacter pour en savoir plus →](#)

Modalités pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2I, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

* nous consulter pour la faisabilité en distanciel

** ratio variable selon le cours suivi

Accessibilité aux personnes en situation de handicap

Détails de la session

Du 4 janvier 2027 au 8 janvier 2027 (5 jours / 35 heures)

Nancy

Du 4 janvier 2027 au 8 janvier 2027

Nancy

- 4 janvier 2027 ----- 9h00 – 15h00
- 5 janvier 2027 ----- 9h00 – 15h00
- 6 janvier 2027 ----- 9h00 – 15h00
- 7 janvier 2027 ----- 9h00 – 15h00
- 8 janvier 2027 ----- 9h00 – 15h00