DAWAN

Plan de la formation

www.dawan.fr

Formation Analyse de risques / PSSI / procédures / sensibilisation

Durée :	3 jours (21 heures)
Tarif inter-entreprises :	2 475,00 € HT (Présentiel) 1 980,00 € HT (Distanciel)
Public :	Administrateur système
Pré-requis :	Connaissances solides en administration système Linux/Windows Notions de base en réseaux (TCP/IP, VLAN, pare-feu) Compréhension générale de la sécurité informatique (CIA triad, IAM, cryptographie de base)
Objectifs :	Comprendre les fondamentaux de la gestion des risques SSI et savoir conduire une analyse de risques opérationnelle - Concevoir et structurer une Politique de Sécurité des Systèmes d'Information (PSSI) adaptée à son contexte - Rédiger des procédures techniques de sécurité exploitables par les équipes d'administration - Concevoir et animer des actions de sensibilisation à la sécurité à destination de différents publics - Articuler l'ensemble dans une démarche cohérente conforme aux référentiels ISO 27001/27005 et au RGS

Méthode pédagogique :	### Atelier fil rouge Un SI fictif réaliste (PME hybride on-premise/cloud, 150 postes, multi-sites) traverse les 3 jours. Chaque bloc produit un livrable concret qui s'appuie sur le précédent, simulant une démarche SSI complète de bout en bout — de l'analyse de risques au plan de sensibilisation. ### Études de cas réels Des incidents publics anonymisés (sources : ANSSI, ENISA, CERT-FR) sont introduits à des moments clés pour ancrer les concepts dans l'opérationnel et alimenter des échanges critiques entre apprenants. ### Apport magistral interactif Séquences courtes (30–45 min max), ponctuées de questions ouvertes et de mises en situation. Les concepts abstraits sont systématiquement illustrés par des exemples tirés des environnements Linux/Windows/réseau familiers aux profils AIS. ### Rédaction technique guidée Gabarits fournis (PSSI, procédures), production en autonomie, puis relecture critique collective. Objectif : des documents opposables, maintenables, directement exploitables en production ou auditables par un tiers. ### Simulation de phishing (GoPhish) Les apprenants configurent un scénario complet côté attaquant — template, ciblage, analyse des résultats. L'exploitation pédagogique des résultats (transformer un taux de clic en levier de sensibilisation sans culpabiliser) est traitée explicitement. ### Mise en situation finale Chaque apprenant anime un module de sensibilisation de 15 minutes devant ses pairs jouant le rôle d'utilisateurs non-techniciens. Débriefing collectif sur le fond et la forme. ### Environnement technique * Référentiels : ISO 27005, ISO 27002:2022, EBIOS RM, RGS, guides ANSSI * Outils : GoPhish, gabarits Markdown/ODT versionnables sous Git, quiz interactif * Poste : Linux recommandé — exemples sous Debian/Ubuntu et RHEL/Rocky
Modalités pédagogiques, techniques et d’encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l’Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l’environnement adéquat. • Un formateur expert.

Modalité d'évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.
Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
Référence :	CYB102990-F
Note de satisfaction des participants :	Pas de données disponibles
Contacts :	commercial@dawan.fr - 09 72 37 73 73
Modalités d'accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
Délais d'accès :	Variable selon le type de financement.
Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

Jour 1 — Analyse de risques SSI : concepts, méthodes et mise en pratique

Bloc 1 — Fondamentaux de la gestion des risques SSI

- Rappel des concepts clés : menace, vulnérabilité, risque, impact, vraisemblance, risque résiduel
- Cadre normatif : ISO 27005, ISO 31000, lien avec ISO 27001 et le RGS (Référentiel Général de Sécurité)
- Positionnement de l'analyse de risques dans le cycle SMSI (Plan-Do-Check-Act)
- Rôles et responsabilités : RSSI, administrateur, MOA/MOE — qui fait quoi dans la démarche ?
- Panorama des méthodes : EBIOS Risk Manager, MEHARI, OCTAVE — critères de choix selon le contexte organisationnel

Atelier fil rouge : Prise de contexte d'un SI fictif (PME industrielle) — identification des enjeux, des parties prenantes et des contraintes réglementaires applicables

Bloc 2 — Identification et cartographie des actifs

- Définition du périmètre et du contexte de l'analyse
- Typologies d'actifs : primaires (processus, données) et secondaires (matériels, logiciels, réseaux, locaux, RH)
- Méthode d'inventaire et de valorisation des actifs — sensibilité DICP (Disponibilité, Intégrité, Confidentialité, Preuve)
- Identification des dépendances entre actifs et cartographie des flux d'information
- Propriétaires d'actifs : désignation, responsabilités, articulation avec la gouvernance SI

Atelier fil rouge : Construction d'un inventaire d'actifs commenté et d'une cartographie de dépendances pour le SI fictif — exploitation sous forme de tableau structuré

Bloc 3 — Appréciation des risques : analyse, évaluation, priorisation

- Recensement des menaces pertinentes : sources humaines, environnementales, techniques
- Identification des vulnérabilités associées aux actifs inventoriés (CVE, configurations, procédures manquantes)
- Évaluation qualitative vs quantitative : matrices d'impact et de vraisemblance, scoring
- Construction de scénarios de risques (EBIOS RM : sources de risque, objets visés, modes opératoires)
- Priorisation et seuils de tolérance — notion d'appétence au risque et de risque inacceptable
- Risques résiduels après mesures existantes — arbitrages acceptation / traitement / transfert / évitement

Atelier fil rouge : Analyse de 5 scénarios de risques sur le SI fictif — positionnement dans une matrice, identification des risques inacceptables et proposition de première hiérarchisation

Jour 2 — PSSI et procédures de sécurité : structuration et rédaction

Bloc 4 — Concevoir et rédiger une PSSI

- Définition et rôle de la PSSI : document stratégique vs opérationnel — ce que la PSSI est, et ce qu'elle n'est pas

- Architecture documentaire SSI : PSSI → politiques thématiques → procédures → modes opératoires
- Contenu type d'une PSSI : périmètre, objectifs, principes directeurs, responsabilités, exigences de sécurité, sanctions
- Alignement avec ISO 27001 Annexe A et les contrôles de sécurité (ISO 27002:2022)
- Cycle de vie de la PSSI : approbation, diffusion, révision périodique, gestion des exceptions
- PSSI dans les environnements régulés : OIV/OSE (NIS2), RGPD, secteur santé (PGSSI-S)

Atelier fil rouge : Rédaction collaborative d'une PSSI synthétique (10 pages) pour le SI fictif — structure, principes directeurs, exigences par domaine (accès, sauvegarde, gestion des incidents, mobilité)

Bloc 5 — Rédiger des procédures techniques de sécurité

- Distinction procédure / mode opératoire / runbook — usages respectifs en environnement d'administration
- Structure type d'une procédure : objet, domaine d'application, références, rôles, étapes, contrôles, révisions
- Domaines couverts : gestion des comptes et des droits, durcissement des systèmes (hardening), gestion des correctifs, sauvegarde/restauration, gestion des incidents, journalisation et supervision
- Écrire pour l'opérationnel : niveau de détail, langage précis, reproductibilité, vérifiabilité
- Versionnement et traçabilité des procédures — intégration dans un outil de gestion documentaire (Wiki, Git, ITSM)
- Lien entre procédures et plan de traitement des risques identifiés en Jour 1

Atelier fil rouge : Rédaction de trois procédures techniques complètes pour le SI fictif — gestion des comptes administrateurs, procédure de patching mensuel, procédure de réponse à un incident de sécurité de niveau 1

Bloc 6 — Plan de traitement des risques et indicateurs de suivi

- Définir les actions de traitement : mesures organisationnelles, techniques, juridiques
- Relier chaque action aux contrôles ISO 27002 correspondants et aux procédures rédigées
- Priorisation des actions : criticité, coût, délai de mise en œuvre, responsable
- Construction d'un tableau de bord SSI minimal : indicateurs de pilotage (KPI/KRI), fréquence de remontée

- Revue des risques résiduels post-traitement — boucle de rétroaction vers la PSSI
- Reporting à la direction : synthèse exécutive, formulation orientée décision

Atelier fil rouge : Élaboration d'un plan de traitement des risques sur 6 mois pour le SI fictif — tableau priorisé avec responsables, délais et indicateurs de suivi associés

Jour 3 — Sensibilisation à la sécurité : conception, animation et évaluation

Bloc 7 — Comprendre les enjeux humains de la sécurité

- Le facteur humain comme principale surface d'attaque : phishing, ingénierie sociale, erreur opérationnelle
- Psychologie de la sécurité : biais cognitifs, résistance au changement, notion de sécurité perçue vs sécurité réelle
- Panorama des incidents liés au comportement humain : études de cas concrets (ransomware, fuite de données, sabotage interne)
- Rôle de l'administrateur dans la culture sécurité : exemplarité, remontée d'incidents, posture de conseil
- Cadre réglementaire de la sensibilisation : obligations RGPD (Art. 39), ISO 27001 (§7.3), ANSSI recommandations

Atelier fil rouge : Analyse de trois incidents réels anonymisés — identification des défaillances humaines, des signaux faibles ignorés, et des mesures de sensibilisation qui auraient pu les prévenir

Bloc 8 — Concevoir un programme de sensibilisation

- Définir les publics cibles et leurs niveaux d'exposition : direction, utilisateurs métiers, équipes techniques, prestataires
- Cartographie des comportements à risque par profil — gap analysis entre comportement actuel et comportement cible
- Formats de sensibilisation : e-learning, ateliers présentiel, campagnes de phishing simulé, affiches, newsletters SSI, serious games
- Planification annuelle d'un plan de sensibilisation : thèmes, supports, fréquence, canaux de diffusion
- Indicateurs d'efficacité : taux de clic sur phishing simulé, taux de complétion e-learning, remontées d'incidents, quiz de connaissance avant/après
- Budget et ressources : internalisation vs externalisation, outils disponibles (MISP, GoPhish, plateformes LMS)

Atelier fil rouge : Conception d'un plan de sensibilisation annuel pour le SI fictif — définition des publics, choix des formats, planning trimestriel, indicateurs d'évaluation

Bloc 9 — Produire et animer des supports de sensibilisation

- Règles de communication efficace en sécurité : message clair, ancrage dans le quotidien, ton adapté au public
- Conception d'un support de sensibilisation : structure, visuels, exemples concrets, appel à l'action
- Animation d'un atelier de sensibilisation : techniques de facilitation, gestion des objections, retour d'expérience
- Campagne de phishing simulé : cadre éthique, déploiement technique (GoPhish), exploitation pédagogique des résultats
- Intégration de la sensibilisation dans l'onboarding des nouveaux arrivants et dans les processus RH
- Mesure de la maturité sécurité des utilisateurs dans le temps — boucle d'amélioration continue

Atelier fil rouge final : Conception et présentation d'un module de sensibilisation de 15 minutes destiné à des utilisateurs non-techniciens — scénario basé sur le SI fictif, support visuel, quiz d'évaluation inclus — restitution devant le groupe avec débriefing collectif