

FICHE • PSSI & GOUVERNANCE

Votre PSSI en 7 étapes

Pour gagner la confiance de vos clients et de vos fournisseurs : sept étapes avec votre équipe IT, une PSSI-cadre et cinq annexes, 20 à 30 h de travail sur 10 à 12 semaines, séances en visioconférence.

Avant l'étape 1 : un échange de cadrage gratuit pour fixer le périmètre, puis un état des lieux de vos configurations relevé en lecture.

01

ÉTAPE 1 • 2 À 3 H

Législation et gouvernance



- Vos obligations : RGPD, NIS2 et ReCyF de l'ANSSI, RGS, référentiels de votre secteur
- Qui porte la sécurité, qui décide, ce qu'on exige des fournisseurs
- Échelles de vraisemblance et de gravité, convenues avec vous

Livable : Matrice d'obligations, rôles, exigences fournisseurs, plan de sensibilisation, feuille de route RGPD

02

ÉTAPE 2 • 3 À 6 H, EN UNE OU DEUX SÉANCES

Risques et menaces



- Rançongiciel, compromission de messagerie, fraude au virement, fuite de données
- Analyse de risque fondée sur EBIOS RM, la méthode de l'ANSSI
- Valeurs métier et biens supports, événements redoutés, scénarios cotés

Livable : Cartographie des valeurs métier et des biens supports, cinq scénarios cotés, plan de traitement

03

ÉTAPE 3 • ENVIRON 3 H

Maintien en condition de sécurité



- Inventaire des actifs et des systèmes en fin de support
- Correctifs : fenêtres de maintenance et correctifs d'urgence
- Sauvegardes 3-2-1, test de restauration, plan de reprise

Livable : Procédure de maintien, trois indicateurs, volet informatique du PCA et PV du test de restauration

04

ÉTAPE 4 • 3 À 4 H

Identités et contrôle d'accès



- Authentification multifacteur, comptes à privilèges et partagés
- Arrivée, départ, mutation, et revue périodique des droits
- Charte informatique : les règles d'usage de chaque utilisateur

Livable : Politique d'accès, arrivées et départs, charte informatique

05

ÉTAPE 5 • 3 À 5 H

Durcissement des systèmes



- Postes de travail, serveurs et annuaire, équipements réseau
- Messagerie : SPF, DKIM, DMARC, filtrage des pièces jointes
- Écarts mesurés sur l'état des lieux relevé avant l'étape 1

Livable : Configurations de référence et écarts priorités

06

ÉTAPE 6 • 3 À 4 H

Cloisonnement réseau



- Segmentation par usage, par sensibilité et par population
- Accès distants, postes d'administration, wifi invités
- Interconnexions avec vos prestataires

Livable : Cartographie du SI et des prestataires, architecture cible, matrice des flux

07

ÉTAPE 7 • 2 À 3 H, PUIS 1 H DE VALIDATION

Journalisation et incidents



- Quoi journaliser, combien de temps, qui lit les alertes
- Incidents : qui décide, fiches réflexes, CNIL sous 72 h, NIS2
- Risques recotés, plan d'action, PSSI validée par la direction

Livable : Journalisation, procédure d'incident, fiches réflexes, annuaire de crise, registre des violations, plan d'action

VOUS REPARTEZ AVEC

- ✓ La PSSI-cadre, signée par la direction
- ✓ A • Charte informatique
- ✓ B • Directives techniques
- ✓ C • Incidents et crises
- ✓ D • Continuité et reprise (volet informatique du PCA)
- ✓ E • Pilotage et conformité, feuille de route RGPD

Votre équipe : 2 à 3 personnes sur tout le parcours. Direction et RH facultatives en séance ; la direction valide la PSSI.

Durées indicatives, sans surcoût

Une étape peut durer plus longtemps selon votre organisation : le prix de la mission ne change pas.

Déroulé fondé sur les objectifs du ReCyF (ANSSI) et la méthode EBIOS RM. Document d'information, non contractuel.

[Demander un audit gratuit](#)

dmc-defense.com/fr/expertise/pssi