

ANNEXE · PSSI & GOUVERNANCE

Votre PSSI : où chaque sujet est traité

Deux repères pour vous situer dans le dossier remis : ce que produit chacune des 7 étapes, puis l'endroit où votre PSSI traite chaque grand domaine de la PSSIE, la politique de sécurité de référence de l'État (ANSSI). Utile pour répondre à un auditeur ou à un questionnaire d'assurance cyber. Nous citons ce référentiel, sans prétendre à une conformité PSSIE.

Les 7 étapes et votre dossier

ÉTAPE	CE QU'ELLE ALIMENTE
1. Législation et gouvernance	PSSI-cadre, chapitres 1 à 4 ; E4 matrice d'obligations ; E2 prestataires ; A5 sensibilisation ; E7 données personnelles et feuille de route RGPD
2. Risques et menaces	PSSI-cadre, chapitre 5 ; E1 analyse et cartographie des risques ; E3 sécurité dans les projets
3. Maintien en condition de sécurité	B1 inventaire et cartographie des actifs ; B3 correctifs ; annexe D en entier (D1 à D5)
4. Identités et contrôle d'accès	B2 identités et accès ; A1 à A4 et A7 (charte informatique)
5. Durcissement des systèmes	B4 postes de travail et serveurs ; B7 chiffrement ; B9 développement, si vous développez
6. Cloisonnement réseau	B5 réseau et architecture ; B8 sécurité physique
7. Journalisation et incidents	B6 journalisation ; annexe C en entier (C1 à C5) ; A6 signaler un incident ; E5 plan d'action ; E6 audits ; PSSI-cadre, chapitres 6 et 7, puis validation par la direction

Les domaines de la PSSIE de l'État

DOMAINE PSSIE (ANSSI)	OÙ VOTRE PSSI LE TRAITE
Politique, organisation, gouvernance	PSSI-cadre, chapitres 1, 4 et 7 ; E2 prestataires
Intégration de la SSI dans le cycle de vie	PSSI-cadre, chapitre 5 ; E1 analyse de risque ; E3 sécurité dans les projets
Sécurité physique	B8 sécurité physique (locaux et équipements)
Sécurité des réseaux et architecture	B1 cartographie des actifs ; B5 réseau et architecture
Exploitation des systèmes	B2 identités et accès ; B3 correctifs ; B6 journalisation ; B7 chiffrement
Sécurité du poste de travail	B4 postes de travail et serveurs ; charte informatique A1 à A3
Traitement des incidents	Annexe C (C1 à C5) ; A6 signaler un incident
Continuité d'activité	Annexe D (D1 à D5) : bilan d'impact, sauvegardes, plan de reprise, volet informatique du PCA, tests
Conformité, audit, contrôle	PSSI-cadre, chapitre 3 ; E4 matrice d'obligations ; E6 audits ; A7 contrôles

Hors tableau : les centres informatiques (responsabilité partagée avec Microsoft pour une organisation sur Microsoft 365), les produits labellisés, les réseaux interministériels et l'inspection ministérielle (propres à l'État).

Source : PSSIE de l'État, circulaire du 17 juillet 2014 (ANSSI). Document d'information, non contractuel.