Documents Audit AirCyber Bronze : Liste et Conseils

Liste complète des documents obligatoires pour réussir l'audit AirCyber Bronze : PSSI, inventaire, PCA, logs, schémas réseau — ce que l'assesseur vérifie.

La visite de l'**assesseur AirCyber accrédité** est un moment clé du processus de labellisation Bronze qui peut représenter une source de stress inutile si l'entreprise n'a pas anticipé la préparation documentaire en amont. Dans la pratique, la majorité des non-conformités relevées lors des audits ne sont pas liées à l'absence de mesures techniques, mais à l'absence de preuves documentaires : une politique non formalisée, un inventaire non à jour, un test de restauration jamais documenté. Cette liste exhaustive recense l'ensemble des *documents probatoires* que vous devez rassembler avant l'audit, organisés par domaine de sécurité et annotés avec leur niveau AirCyber requis. Pour chaque document, vous trouverez son nom exact, son contenu attendu et des conseils pratiques pour le produire rapidement. Elle complète le guide complet de la labellisation et la checklist des 44 mesures ANSSI.

Points clés à retenir

• La conformité ISO 27001 est un processus continu, pas une certification ponctuelle

• L'implication de la direction est le facteur clé de succès de tout SMSI

• Les 93 contrôles de l'Annexe A couvrent tous les domaines de la sécurité organisationnelle

À RETENIR

À retenir

L'assesseur AirCyber ne vérifie pas seulement l'existence des documents : il s'assure qu'ils sont datés, signés par la direction, diffusés au personnel concerné et effectivement appliqués. Un document générique non adapté à votre contexte peut être refusé. Privilégiez la qualité et la pertinence sur la quantité.

Documents de politique de sécurité et organisation

Ce sont les fondations documentaires de votre démarche. Sans eux, aucun autre domaine ne peut être validé. Ils doivent être **signés par le dirigeant ou le responsable habilité**, datés, versionnés et accessible à l'ensemble des collaborateurs concernés.

⚡ **Retour terrain**

J'ai réalisé un audit de conformité PCI-DSS pour un e-commerçant de taille moyenne. La surprise : leur prestataire de paiement gérait effectivement la conformité PCI côté serveur, mais les formulaires de carte côté client passaient par leurs propres serveurs via un JavaScript personnalisé — introduisant un scope PCI non déclaré. La remédiation a nécessité une migration vers un formulaire de paiement hébergé (redirect ou iFrame).

1. Politique de Sécurité des Systèmes d'Information (PSSI)

Niveau requis : Bronze

Contenu attendu : périmètre couvert, objectifs de sécurité, rôles et responsabilités, principes directeurs, sanctions en cas de non-respect. La PSSI doit être adaptée à votre contexte (taille, secteur, types de données traitées). Longueur typique : 5 à 15 pages.

Conseil : L'ANSSI propose des modèles de PSSI pour PME. Adaptez-le à votre contexte plutôt que de partir de zéro. Prévoir 3 à 5 jours de travail.

2. Charte utilisateurs informatique

Niveau requis : Bronze

Contenu attendu : règles d'utilisation acceptables des ressources informatiques, interdictions explicites (téléchargements non autorisés, usage personnel excessif, partage de mots de passe), conséquences disciplinaires. Doit être signée par chaque employé lors de l'embauche.

Conseil : Intégrez-la au contrat de travail ou faites-la signer séparément avec accusé de réception. L'assesseur peut demander les listes de signatures.

3. Procédure de gestion des incidents de sécurité

Niveau requis : Bronze

Contenu attendu : définition d'un incident, critères d'escalade, contacts d'urgence (interne +

ANSSI CERT-FR), délais de notification aux donneurs d'ordres (notamment Safran), processus de documentation et de retour d'expérience.
Conseil : Gardez ce document court (2-3 pages) et opérationnel. Il doit être imprimable et affiché dans les locaux techniques.

4. Registre des traitements et classification des données
Niveau requis : Bronze (partiel) / Silver (complet)
Contenu attendu : liste des données sensibles traitées (données techniques ITAR/EAR, données contractuelles, données personnelles RGPD), niveau de classification, mesures de protection associées, durée de conservation.
Conseil : Commencez par un tableau simple (Excel ou équivalent) listant vos données par type. Classifiez en trois niveaux : Public / Interne / Confidentiel.

Inventaire des actifs informatiques

L'*inventaire des actifs* est le document le plus souvent manquant ou incomplet lors des audits. Il doit couvrir **100 % des équipements** connectés au réseau de l'entreprise — y compris les équipements industriels (CNC, bancs de test) ayant une interface réseau.

5. Inventaire du matériel informatique
Niveau requis : Bronze
Contenu attendu : pour chaque équipement — nom, type, modèle, numéro de série, adresse IP/MAC, version OS, date d'acquisition, propriétaire, localisation physique, statut (actif/inactif). Couvre les serveurs, postes de travail, laptops, équipements réseau, NAS, imprimantes réseau, équipements industriels connectés.
Conseil : Un scan réseau via des outils comme Nmap ou Advanced IP Scanner peut automatiser la découverte initiale. Planifiez une mise à jour trimestrielle.

6. Inventaire des logiciels et licences

Niveau requis : Bronze

Contenu attendu : liste de tous les logiciels installés sur les postes, version, éditeur, type de licence (perpétuelle/abonnement), date d'expiration de la licence, poste(s) concerné(s). Signaler les logiciels en fin de support (**EOL**).

Conseil : Utilisez un outil d'inventaire automatisé (GLPI, OCS Inventory — tous deux gratuits) pour maintenir cet inventaire à jour.

Plan de continuité et reprise d'activité

Les documents **PCA/PRA** sont évalués à la fois sur leur existence et sur leur caractère opérationnel. Un plan jamais testé sera considéré comme insuffisant par l'assesseur. La preuve des tests de restauration est indispensable.

7. Plan de Reprise d'Activité (PRA)

Niveau requis : Bronze

Contenu attendu : liste des systèmes critiques par ordre de priorité de reprise, *RTO* (Recovery Time Objective) et *RPO* (Recovery Point Objective) cibles pour chaque système, procédures de restauration pas-à-pas, contacts d'urgence, infrastructure de reprise (site backup, cloud).

Conseil : Commencez par les 3 à 5 systèmes les plus critiques pour votre activité. Un PRA imparfait mais testé vaut mieux qu'un PRA parfait jamais mis en pratique.

8. Rapports de tests de restauration

Niveau requis : Bronze

Contenu attendu : date du test, système restauré, données testées, durée de restauration constatée vs objectif, écarts identifiés, actions correctives. Au moins un test par an, idéalement deux.

Conseil : Planifiez le prochain test dès maintenant et documentez-le formellement même si le résultat est imparfait. L'assesseur apprécie la démarche d'amélioration continue.

Gestion des accès et de l'authentification

9. Liste des comptes à privilèges et droits d'accès

Niveau requis : Bronze

Contenu attendu : liste de tous les comptes administrateurs (locaux et de domaine), droits associés, justification métier de ces droits, date de dernière revue. L'assesseur vérifiera qu'il n'existe pas de comptes fantômes (anciens employés).

Conseil : Réalisez une revue des accès complète avant l'audit. Désactivez immédiatement les comptes des personnes ayant quitté l'entreprise.

10. Politique de gestion des mots de passe et MFA

Niveau requis : Bronze

Contenu attendu : paramètres de politique de mots de passe (longueur, complexité, historique, verrouillage), liste des systèmes couverts par le **MFA**, procédure de réinitialisation sécurisée.

Conseil : Exportez les paramètres de la GPO Active Directory (ou équivalent) et joignez-les en annexe. C'est la preuve la plus directe de mise en œuvre.

Architecture réseau et sécurité périmétrique

11. Schémas d'architecture réseau

Niveau requis : Bronze

Contenu attendu : schéma logique et physique du réseau avec toutes les zones (DMZ, réseau bureautique, réseau de production, WiFi), flux autorisés entre zones, emplacement des équipements de sécurité (firewall, IPS, proxy). Doit être à jour.
Conseil : Utilisez draw.io (gratuit) pour créer ou mettre à jour vos schémas. L'assesseur doit pouvoir comprendre votre architecture en 5 minutes.

12. Règles de filtrage du pare-feu
Niveau requis : Bronze (export anonymisé)
Contenu attendu : export ou documentation des règles principales du pare-feu, justification métier de chaque règle autorisant des flux entrants depuis Internet. Les règles "any-any" doivent être expliquées ou supprimées.
Conseil : Ne partagez pas l'export brut en amont de l'audit. Préparez une version synthétique listant les flux entrants et leur justification.

Journalisation et prestataires

13. Politique de journalisation et de rétention des logs
Niveau requis : Bronze
Contenu attendu : liste des équipements journalisés, types d'événements enregistrés, durée de rétention, solution de centralisation (SIEM ou serveur de logs), procédure d'accès et d'analyse des logs.
Conseil : Si vous n'avez pas de SIEM, documentez au minimum la configuration de journalisation des serveurs Windows/Linux et des équipements réseau.

14. Contrats prestataires avec clauses de sécurité
Niveau requis : Bronze
Contenu attendu : pour chaque prestataire ayant accès à votre SI (infogérance, SSII, maintenance industrielle à distance) — contrat incluant des clauses de confidentialité, de

sécurité des accès, de notification d'incident et de restitution des données en fin de contrat.
Conseil : L'assesseur peut demander à voir un ou deux contrats types. Assurez-vous que les accès distants des prestataires sont tracés et révocables.

Comment organiser votre dossier documentaire

Organisez ces documents dans un **dossier de preuve structuré**, par exemple sur un partage réseau sécurisé ou un espace documentaire dédié. Numérotez chaque document en référence aux mesures AirCyber correspondantes. Préparez une *table de correspondance* indiquant pour chaque mesure ANSSI quel document en constitue la preuve.

Prévoyez également des captures d'écran des configurations système les plus importantes (politique de mots de passe AD, règles de pare-feu, configuration des sauvegardes) : elles constituent une preuve technique complémentaire aux documents organisationnels.

Si vous êtes fournisseur Safran, consultez également notre guide sur l'obligation AirCyber Bronze imposée par Safran à ses fournisseurs. Pour aller plus loin, notre accompagnement AirCyber inclut un accompagnement documentaire complet et la préparation à la visite assesseur. Vous pouvez également consulter notre centre de ressources AirCyber pour accéder à l'ensemble de nos guides pratiques. Pour les aspects de financement, référez-vous à notre article sur les subventions AirCyber disponibles pour les PME.

Le Guide d'Hygiène Informatique de l'ANSSI est disponible gratuitement en ligne et constitue la référence officielle pour comprendre le détail de chaque mesure. Le portail BoostAerospace AirCyber fournit le questionnaire officiel d'auto-évaluation.

FAQ — Documents d'audit AirCyber Bronze

L'assesseur peut-il accéder à nos systèmes durant l'audit ?

Oui, l'assesseur procède généralement à des vérifications techniques directes sur les systèmes en présence du responsable technique. Il peut consulter les configurations du pare-feu, les paramètres de la politique de mots de passe Active Directory, les registres de sauvegarde et les journaux d'événements. Ces vérifications techniques complètent la revue documentaire et permettent de s'assurer de l'effectivité des mesures.

Que se passe-t-il si certains documents sont en cours de rédaction au moment de l'audit ?

L'assesseur peut prendre en compte des documents en version "draft" signalés comme tels, à condition qu'ils soient substantiellement complets et qu'un plan de finalisation soit formalisé. Les documents critiques (PSSI, charte utilisateurs, PRA) doivent cependant être finalisés avant l'audit pour éviter un avis de non-conformité. Il est préférable de reporter l'audit de quelques semaines plutôt que de se présenter avec un dossier incomplet.

Quelle est la durée de validité des documents présentés lors de l'audit ?

Les documents doivent être à jour au moment de l'audit. Une PSSI datant de plus de 2 ans sans révision sera considérée comme obsolète. L'inventaire des actifs doit refléter l'état actuel du parc. Les rapports de test de restauration doivent dater de moins de 12 mois. Après l'obtention du label Bronze (valide 2 ans), une revue documentaire annuelle est recommandée pour maintenir la conformité.

Mise en œuvre pratique : étapes et livrables

La conformité réglementaire génère une documentation substantielle qui doit être maintenue à jour et accessible lors des audits. Une organisation structurée de ces livrables simplifie considérablement les exercices de conformité et réduit le temps consacré à leur préparation.

Livrables documentaires essentiels

Quel que soit le référentiel de conformité concerné, les livrables fondamentaux incluent : un registre des traitements (obligatoire RGPD, utile pour tout SMSI) maintenu par le DPO ou le RSSI ; une politique de sécurité de l'information (PSI ou PSSI) approuvée par la direction et diffusée à tous les collaborateurs ; des procédures opérationnelles documentées pour les processus critiques (gestion des incidents, accès privilégiés, sauvegardes) ; un plan de continuité d'activité (PCA) testé annuellement ; et des rapports d'audit internes et de revue de direction formalisés. Ces documents constituent le «squelette» du SMSI et sont systématiquement vérifiés lors des audits de certification.

Gouvernance et responsabilités

La conformité réglementaire est un effort collectif qui ne peut pas reposer uniquement sur le RSSI ou le DPO. Une gouvernance efficace définit clairement les rôles : le COMEX assume la responsabilité globale de la conformité (risque financier et réputationnel) ; les DSI et RSSI mettent en œuvre les mesures techniques ; les métiers identifient les données et processus critiques à protéger ; et les DPO/compliance officers assurent la cohérence réglementaire. Les comités de sécurité trimestriels, impliquant toutes ces parties prenantes, garantissent l'alignement entre les exigences réglementaires et les capacités opérationnelles de l'organisation. Le suivi des actions de remédiation dans un outil de GRC (Governance, Risk & Compliance) formalise ce processus et facilite la production des preuves d'audit.

Sanction et contrôle : ce que les autorités vérifient

Comprendre les priorités de contrôle des autorités de régulation permet aux organisations de concentrer leurs efforts sur les domaines qui font l'objet d'une surveillance accrue. Les autorités de supervision (CNIL, ANSSI, ACP pour le secteur bancaire, HAS pour le secteur santé) publient régulièrement leurs priorités de contrôle.

Priorités de contrôle 2025-2026

Les domaines prioritaires identifiés par les autorités françaises pour 2025-2026 : la sécurité des données de santé (contrôles HDS en forte augmentation suite aux incidents hospitaliers) ; l'IA et le traitement des données personnelles (CNIL a annoncé 300 mises en demeure liées à l'IA en 2025) ; les sous-traitants et tiers (vérification des DPA et des audits de sécurité des fournisseurs) ; et la notification des violations de données dans les délais légaux (72h RGPD, 24h NIS 2 pour les entités essentielles). Les organisations qui documentent proactivement leur conformité dans ces domaines réduisent significativement leur exposition aux sanctions et bénéficient généralement d'une procédure d'audit moins contraignante.

Programme de préparation aux audits

Un programme structuré de préparation aux audits réduit le stress et améliore les résultats. Douze mois avant un audit de certification : gap analysis interne pour identifier les non-conformités. Six mois avant : corrections des écarts majeurs et préparation de la documentation. Trois mois avant : audit blanc interne conduit par un consultant externe indépendant. Un mois avant : formation des équipes sur les procédures et livrables à présenter. Cette approche systématique, validée par des centaines d'organisations certifiées ISO 27001, transforme l'audit de certification d'une épreuve redoutée en une validation formelle d'un travail déjà accompli.

Synthèse et feuille de route conformité

La conformité réglementaire est un processus continu, non un projet ponctuel. Les organisations qui abordent ISO 27001, NIS 2, RGPD ou HDS comme des certifications à obtenir une fois pour toutes échouent systématiquement lors des audits de renouvellement. La clé du succès est l'intégration des exigences réglementaires dans les processus opérationnels quotidiens, non leur traitement comme des obligations externes.

En pratique, les organisations matures en matière de conformité fonctionnent avec un SMSI vivant : des revues de direction trimestrielles, un audit interne annuel, des exercices de gestion de crise bi-annuels, et une veille réglementaire hebdomadaire. Le coût de la conformité maintenue en continu est significativement inférieur au coût d'une remise à niveau précipitée avant un audit ou une notification de violation. Les amendes CNIL, les pénalités NIS 2, et les pertes de contrats liées à une non-conformité documentée représentent des risques financiers et réputationnels mesurables que la gouvernance de direction doit intégrer dans l'analyse des risques métier.

Points d'attention avancés pour les auditeurs et RSSI

Au-delà de la conformité de surface, les auditeurs expérimentés et les RSSI cherchent à évaluer la robustesse réelle du dispositif de sécurité. Ce niveau d'analyse requiert de dépasser la vérification documentaire pour s'intéresser à l'efficacité opérationnelle des contrôles.

Pièges courants dans les audits de conformité

Plusieurs patterns d'échec reviennent régulièrement lors des audits de renouvellement. La conformité sur papier sans effectivité opérationnelle : des politiques formalisées mais non appliquées, des procédures documentées mais inconnues des équipes, des contrôles déclarés actifs mais non supervisés. La dérive post-certification : les organisations qui traitent la certification comme une fin en soi plutôt que comme un jalons d'un processus continu connaissent systématiquement une dégradation de leur posture sécurité entre deux audits. La

gestion insuffisante des tiers : plus de 60% des violations impliquent un fournisseur ou un prestataire, mais les contrats de sous-traitance et les audits tiers sont souvent les parents pauvres des programmes de conformité. Adresser ces trois points avant l'audit réduit significativement le risque de non-conformité majeure.

Métriques de maturité à présenter en audit

Les auditeurs modernes s'intéressent aux indicateurs de fonctionnement réel du SMSI plutôt qu'à la simple existence des documents. Préparer : statistiques de gestion des incidents sur 12 mois (nombre, délai de traitement, taux de récidive) démontrant une amélioration continue ; résultats des exercices de continuité avec les actions correctives entreprises ; données de sensibilisation (taux de participation aux formations, taux d'échec aux simulations de phishing) ; et résultats des audits internes avec suivi des actions de remédiation. Ces métriques transforment l'audit en démonstration de la maturité de l'organisation plutôt qu'en exercice de conformité documentaire, et constituent la meilleure défense contre les questions inattendues des auditeurs sur l'efficacité opérationnelle des contrôles.

Checklist de mise en œuvre et points de contrôle

La mise en pratique des recommandations de cet article nécessite une approche structurée. Cette checklist synthétise les points de contrôle essentiels pour évaluer l'état d'avancement de votre déploiement et identifier les actions prioritaires.

Phase de préparation et d'inventaire

Avant toute action technique, constituer un inventaire précis est indispensable. Les éléments à recenser : cartographie exhaustive des actifs concernés (systèmes, applications, flux de données) avec leur criticité métier associée ; identification des propriétaires techniques et fonctionnels pour chaque actif ; évaluation du niveau de maturité actuel à partir des référentiels reconnus (CIS Controls, ISO 27001, NIST CSF) ; et documentation des dépendances entre composants pour

anticiper les impacts des modifications. Un inventaire incomplet génère des angles morts qui deviennent des vecteurs d'attaque exploitables par des acteurs malveillants disposant d'informations accessibles publiquement (OSINT, Shodan, LinkedIn).

Phase de déploiement et validation

Le déploiement progressif réduit les risques d'interruption de service et facilite la détection des régressions. Adopter un modèle de déploiement par vagues (wave deployment) : d'abord les environnements de développement et de test pour valider les configurations, ensuite les systèmes non-critiques en production, enfin les systèmes critiques lors de fenêtres de maintenance planifiées. Chaque vague s'accompagne d'une validation fonctionnelle complète et d'une période d'observation des métriques de performance et de sécurité. Un plan de retour arrière documenté et testé est obligatoire avant toute opération sur un système critique. Les critères de succès doivent être définis avant le déploiement, non après — un taux de faux positifs inférieur à 5% pour les alertes de sécurité, une disponibilité maintenue au niveau SLA contractuel, et l'absence d'incidents de sécurité liés aux modifications.

Phase de supervision et d'amélioration continue

La mise en place d'indicateurs de suivi permet de mesurer l'efficacité des mesures déployées et de justifier leur maintien auprès de la direction. Tableau de bord mensuel recommandé : nombre d'alertes générées par catégorie (critique, majeur, mineur) avec tendance sur 6 mois ; taux de couverture des actifs critiques par les contrôles de sécurité ; délai moyen de remédiation des vulnérabilités par sévérité CVSS ; et résultats des tests de régression mensuels sur les règles de détection. Ce tableau de bord, présenté en comité de sécurité, constitue la base d'un dialogue constructif entre les équipes techniques et le management sur les priorités d'investissement en cybersécurité.