# Financement AirCyber PME : Subventions et Aides 2026

> Tout savoir sur le financement AirCyber pour les PME : France 2030, aides régionales, coût réel du diagnostic et étapes de la demande de subvention.

Obtenir la **labellisation AirCyber Bronze** représente un investissement significatif pour une PME aéronautique — généralement entre 15 000 et 50 000 € HT selon l'ampleur des écarts identifiés lors du diagnostic initial. La bonne nouvelle, encore trop souvent ignorée des entreprises concernées, est que de nombreux dispositifs de *subvention* permettent de réduire ce coût de 50 % à 70 %, voire davantage dans certains cas grâce aux cumuls possibles entre aides nationales et régionales. France 2030 Cyber PME, les aides des clusters aéronautiques régionaux et les dispositifs sectoriels GIFAS constituent un écosystème de financement méconnu que les PME n'utilisent que trop peu, souvent faute d'information sur les modalités d'accès. Ce guide détaille les dispositifs disponibles en 2026, les montants accessibles, les conditions d'éligibilité et les étapes concrètes pour déposer votre demande de financement. Il complète notre guide complet de la labellisation AirCyber Bronze et notre article sur l'obligation AirCyber Bronze chez Safran.

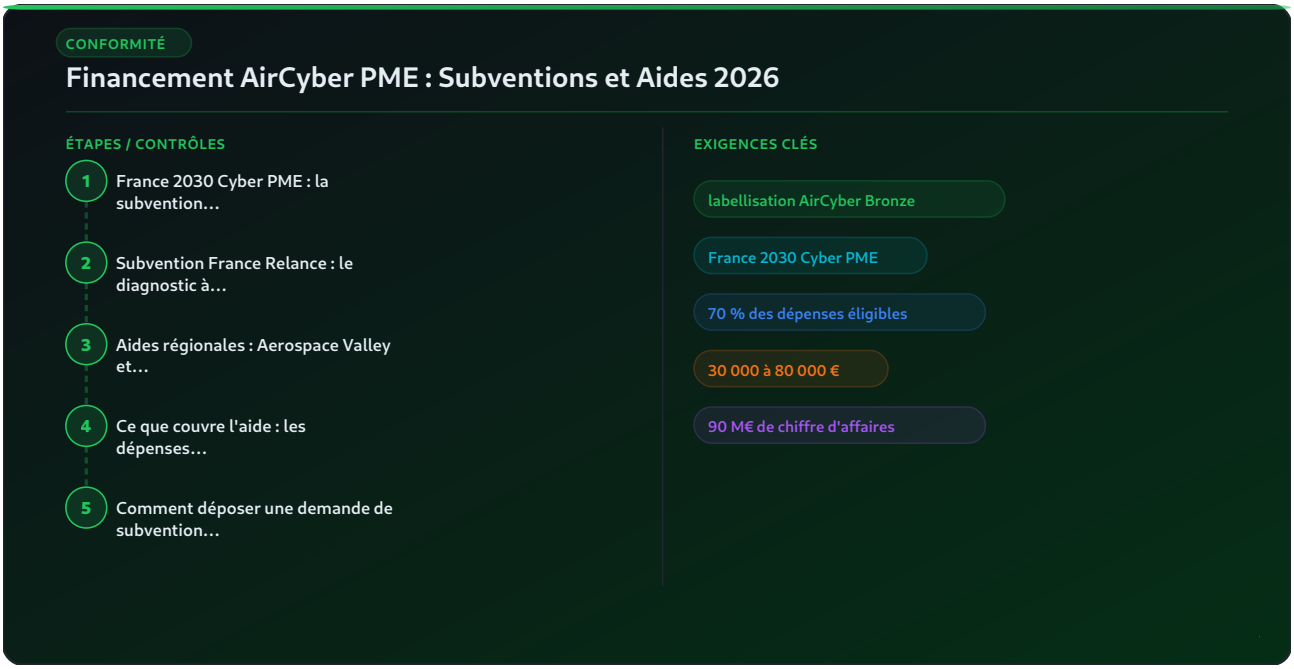
### Points clés à retenir

- 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

Le coût réel du diagnostic AirCyber Bronze est d'environ 4 400 € HT après subvention France Relance (50 %). France 2030 Cyber PME permet ensuite de financer jusqu'à 70 % du plan de sécurisation, pour des montants de 30 000 à 80 000 €. Ces dispositifs sont cumulables sous conditions.




## France 2030 Cyber PME : la subvention principale

Le dispositif **France 2030 Cyber PME** est le mécanisme de financement le plus important disponible pour les entreprises engagées dans une démarche AirCyber. Il s'inscrit dans le volet cybersécurité du plan France 2030, doté de 1 milliard d'euros sur cinq ans.

> ⚡ **Retour terrain**
>
> Dans mes missions de conformité, j'observe que les entreprises sous-estiment systématiquement le délai de mise en œuvre des mesures techniques. Les mesures organisationnelles (politiques, procédures) s'écrivent en semaines ; les mesures techniques (segmentation réseau, chiffrement, MFA) se déploient en mois. Pour un plan de mise en conformité réaliste, je multiplie toujours les estimations initiales des équipes IT par 2,5 — et je n'ai jamais eu à réduire ce coefficient.

Le dispositif couvre jusqu'à **70 % des dépenses éligibles** de sécurisation informatique, pour des montants allant de **30 000 à 80 000 €** par entreprise bénéficiaire. Les dépenses éligibles incluent : le diagnostic de sécurité (auto-évaluation et audit assesseur), le plan de remédiation, la mise en œuvre des solutions techniques (pare-feu, EDR, solution de sauvegarde, MFA), la formation du personnel et l'accompagnement par un prestataire de sécurité qualifié.

Les conditions d'éligibilité sont les suivantes :

Entreprise de moins de **90 M€ de chiffre d'affaires**

Appartenance à un secteur stratégique (aéronautique, défense, spatial, santé, énergie — AirCyber est expressément mentionné)

Engagement dans une démarche de labellisation ou de certification reconnue (AirCyber, ISO 27001, HDS…)

Recours à un prestataire qualifié (assesseur AirCyber accrédité ou PAMS qualifié ANSSI)

L'instruction du dossier est réalisée par **BpiFrance** en lien avec l'ANSSI. Le délai de traitement est généralement de 6 à 10 semaines. La subvention est versée en deux tranches : 40 % à la notification d'attribution, 60 % à la présentation des justificatifs de réalisation.

## Subvention France Relance : le diagnostic à 50 %

Le dispositif *France Relance* dans sa déclinaison cybersécurité permet de subventionner à hauteur de **50 %** le coût du diagnostic de sécurité initial. Pour le diagnostic AirCyber, le coût standard est d'environ **8 800 € HT** — la subvention ramène donc votre reste à charge à environ **4 400 € HT**.

Ce dispositif est plus simple à mobiliser que France 2030 : il ne nécessite pas de dossier complexe, la démarche est initiée directement auprès d'un assesseur AirCyber accrédité qui vous accompagne dans la demande. La subvention est versée après réalisation du diagnostic et remise du rapport.

Ce financement est cumulable avec France 2030 : vous pouvez d'abord obtenir la subvention France Relance pour le diagnostic, puis solliciter France 2030 pour financer le plan de remédiation. Vérifiez cependant les règles de cumul en vigueur au moment de votre demande auprès de BpiFrance.

## Aides régionales : Aerospace Valley et Normandie AeroEspace

En complément des dispositifs nationaux, des aides régionales ciblées sont disponibles dans les deux grandes régions de la filière aéronautique française.

### Aerospace Valley — Nouvelle-Aquitaine et Occitanie

**Aerospace Valley**, le pôle de compétitivité aéronautique et spatial du sud-ouest, dispose de financements dédiés à la cybersécurité des PME membres. Il propose des subventions complémentaires allant de 5 000 à 15 000 € pour les entreprises membres engagées dans une démarche AirCyber. Ces aides peuvent couvrir une partie des dépenses non prises en charge par France 2030 (formation, acquisition de solutions spécifiques).

Le pôle organise également des *workshops* collectifs gratuits de préparation à AirCyber, réduisant le coût de l'accompagnement pour les PME participantes. Contactez directement Aerospace Valley pour connaître les dispositifs en cours et les dates des prochaines sessions.

### Normandie AeroEspace

**Normandie AeroEspace**, le cluster aéronautique normand, propose des aides similaires pour les entreprises de la région engagées dans AirCyber. Les aides régionales normandes en matière de cybersécurité industrielle peuvent atteindre 20 000 € dans le cadre des *SRDEII* (Schémas Régionaux de Développement Économique, d'Innovation et d'Internationalisation). Rapprochez-vous de votre conseiller régional pour connaître les modalités exactes.

## Ce que couvre l'aide : les dépenses éligibles en détail

Pour maximiser votre demande de financement, il est essentiel de comprendre précisément quelles dépenses sont éligibles et comment les documenter.

**Diagnostic AirCyber** (auto-évaluation + audit assesseur) : 100 % éligible, généralement entre 6 000 et 12 000 € HT selon la taille de l'entreprise. C'est la première dépense à déclarer.

**Plan de remédiation** : 100 % éligible. Cela inclut les prestations de conseil pour définir les actions correctives et rédiger les documents de politique de sécurité. Prévoir 3 000 à 8 000 € HT pour une PME de 20 à 50 personnes.

**Mise en œuvre technique** : 100 % éligible dans la limite du plafond. Cela couvre l'acquisition et le déploiement de solutions de sécurité : **EDR** (1 500 à 5 000 €/an), solution de **sauvegarde chiffrée hors site** (2 000 à 8 000 €), **pare-feu nouvelle génération** (2 000 à 10 000 €), solution de **MFA** (1 000 à 3 000 €/an), **SIEM** ou centralisation des logs (3 000 à 15 000 €).

**Formation et sensibilisation** : éligible à 100 %. Inclut les formations techniques, les exercices de phishing simulé et les sessions de sensibilisation pour le personnel. Prévoir 1 000 à 5 000 € HT.

## Comment déposer une demande de subvention France 2030

Le processus de demande France 2030 Cyber PME se déroule en quatre étapes principales, avec un délai global de 8 à 12 semaines entre le dépôt et la notification.

**Étape 1 — Préparez votre dossier** : rassemblez les éléments suivants — extrait Kbis récent, liasses fiscales des 3 derniers exercices, rapport de diagnostic AirCyber (ou devis d'assesseur si le diagnostic est à venir), plan de sécurisation chiffré et détaillé, courrier ou preuve de l'exigence donneurs d'ordres (notification Safran, clause contractuelle).

**Étape 2 — Déposez sur la plateforme BpiFrance** : le dossier est déposé en ligne sur le portail BpiFrance dédiié au dispositif Cyber PME. Un conseiller BpiFrance de votre région vous est attribué pour accompagner l'instruction.

**Étape 3 — Instruction et audition** : un expert ANSSI mandate peut être sollicité pour valider la pertinence technique du plan de sécurisation. Dans certains cas, un entretien téléphonique avec votre conseiller BpiFrance est organisé.

**Étape 4 — Notification et versement** : après notification, signez la convention de subvention et démarrez les travaux. Conservez tous les justificatifs (factures, PV de réception, rapports de formation) pour le solde.

Notre accompagnement AirCyber inclut une assistance au montage des dossiers de financement France 2030 et France Relance. Consultez notre centre de ressources AirCyber pour l'ensemble des guides pratiques de la démarche, notamment la checklist des 44 mesures ANSSI et les documents à préparer pour l'audit.

Pour en savoir plus sur les exigences techniques à satisfaire, référez-vous au Guide d'Hygiène Informatique de l'ANSSI et au portail officiel AirCyber BoostAerospace.

# FAQ — Financement AirCyber PME

## Quelles sont les conditions d'éligibilité à France 2030 Cyber PME ?

Les conditions principales sont : chiffre d'affaires inférieur à 90 M€, appartenance à un secteur stratégique (dont l'aéronautique), engagement dans une démarche de labellisation reconnue (AirCyber, ISO 27001, etc.) et recours à un prestataire qualifié. Les auto-entrepreneurs et holdings pures ne sont généralement pas éligibles. Une vérification de votre éligibilité est réalisée lors du premier contact avec votre conseiller BpiFrance.

## Peut-on cumuler France Relance, France 2030 et les aides régionales ?

En principe, oui. Le cumul est possible dans la limite de 100 % des dépenses éligibles (vous ne pouvez pas percevoir plus que ce que vous avez dépensé). Dans la pratique, France Relance finance le diagnostic initial (50 %), France 2030 finance le plan de sécurisation (jusqu'à 70 %) et les aides régionales complètent sur les dépenses résiduelles. Chaque dossier étant instruit séparément, la cohérence doit être assurée dans les justificatifs présentés à chaque financeur.

## L'aide est-elle versée avant ou après les travaux ?

Pour France 2030, une avance de 40 % est versée à la notification de la subvention, le solde (60 %) étant versé sur justificatifs de réalisation. Pour France Relance diagnostic, le versement intervient après réalisation du diagnostic et remise du rapport d'assesseur. Prévoyez donc une trésorerie suffisante pour préfinancer les dépenses, en particulier pour la phase de mise en œuvre technique.

## Pour aller plus loin : Mise en œuvre pratique

La conformité réglementaire nécessite une approche structurée et documentée. Ces ressources complémentaires permettent d'approfondir les points techniques et juridiques abordés dans cet article.

### Outils d'auto-évaluation

**ANSSI — Outil d'évaluation cybersécurité** — Le Diagnostic de Cybersécurité de l'ANSSI permet d'évaluer le niveau de maturité de votre organisation sur 5 domaines clés. Gratuit et disponible sur diagnostic.ssi.gouv.fr.

**ENISA — Outil d'auto-évaluation NIS2** — Questionnaire structuré pour identifier les exigences applicables à votre secteur et votre taille d'organisation.

**Logiciels GRC** — Des solutions comme Vanta, Drata ou TrustCloud automatisent la collecte de preuves de conformité et accélèrent les processus d'audit.

### Documentation à produire en priorité

Politique de Sécurité du Système d'Information (PSSI) — document fondateur

Registre des activités de traitement (RGPD, article 30)

Analyse d'impact relative à la protection des données (AIPD/DPIA)

Plan de continuité d'activité (PCA) et plan de reprise d'activité (PRA)

Procédure de gestion des incidents de sécurité (notification ANSSI/CNIL)

### Accompagnement et conseil

La mise en conformité implique souvent une assistance externe pour les organisations ne disposant pas d'expertise interne. Les RSSI externalisés ou les consultants spécialisés en conformité peuvent accélérer significativement le processus, notamment pour la préparation aux audits de certification ISO 27001 ou pour la mise en conformité NIS 2 avec un délai contraint.

## 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.