Certification AERO EXCELLENCE™ : Parcours Bronze, Silver, Gold

Points essentiels

- Le référentiel AERO EXCELLENCE™ V2 comporte huit domaines de contrôle communs aux trois niveaux
- Les niveaux Bronze, Silver et Gold imposent des exigences croissantes sur les mêmes domaines
- Les écarts d'audit les plus fréquents sont documentaires, non techniques : mesures appliquées mais non formalisées
- Une planification anticipée des ressources évite les délais rallongés et les surcoûts d'obtention du label

Obtenir la certification AERO EXCELLENCE™ délivrée par le GIFAS constitue une démarche structurée qui s'articule autour de trois niveaux de maturité progressifs. La certification AERO EXCELLENCE Bronze Silver Gold impose à chaque palier un ensemble de contrôles à satisfaire, répartis sur plusieurs domaines de la cybersécurité : gouvernance organisationnelle, gestion des risques fournisseurs, protection des données techniques, sécurisation des systèmes industriels et réponse aux incidents. Le niveau Bronze pose les fondations essentielles attendues de tout sous-traitant aéronautique, le niveau Silver renforce les exigences documentaires et opérationnelles, tandis que le niveau Gold vise une maturité avancée comparable aux standards ISO 27001. Ce guide détaille les prérequis de chaque parcours, le déroulement de l'audit, les délais moyens d'obtention et les points de vigilance qui font échouer la majorité des candidatures des PME de la filière.

Vue d'ensemble des trois niveaux de certification

Le référentiel AERO EXCELLENCE™ V2 est structuré autour de huit domaines de contrôle communs aux trois niveaux, mais avec un niveau d'exigence croissant. Comprendre cette architecture est essentiel pour planifier sa démarche :

> Lors de nos missions d'accompagnement NIS 2, les écarts les plus fréquents ne sont pas techniques mais documentaires : des mesures en place depuis des années, mais non formalisées, non auditées, et donc indémontrables lors d'un contrôle.
>
> *— Retour terrain, Ayi NEDJIMI Consultants*

Domaine 1 — Gouvernance et organisation : Politique de sécurité, rôles et responsabilités, gestion des risques, sensibilisation.

Domaine 2 — Gestion des actifs : Inventaire du SI, classification des données, gestion du cycle de vie des équipements.

Domaine 3 — Contrôle des accès : Gestion des identités, authentification, gestion des privilèges, comptes de service.

Domaine 4 — Sécurité des systèmes et des réseaux : Configuration sécurisée, mises à jour, segmentation réseau, VPN, pare-feu.

Domaine 5 — Protection des données : Chiffrement, sauvegarde, gestion des supports amovibles, transferts sécurisés.

Domaine 6 — Détection et réponse aux incidents : Journalisation, monitoring, procédures de réponse, notification.

Domaine 7 — Continuité d'activité : PCA/PRA, tests de restauration, gestion de crise.

Domaine 8 — Sécurité de la chaîne d'approvisionnement : Gestion des tiers, clauses contractuelles, évaluation des fournisseurs critiques.

Niveau Bronze — Parcours détaillé (60 contrôles, 3-4 mois)

Gouvernance Bronze : les contrôles incontournables

Le niveau Bronze en gouvernance exige l'existence d'une politique de sécurité de l'information formalisée, approuvée par la direction générale (pas uniquement par le responsable informatique) et communiquée à l'ensemble des collaborateurs. Cette politique doit couvrir a minima : la classification des données, les règles d'utilisation des équipements et des systèmes d'information, les responsabilités en matière de sécurité et les sanctions en cas de manquement.

Un référent sécurité doit être nommé formellement. Dans une PME sans DSI, ce référent peut être le responsable informatique ou même le directeur général, mais son rôle doit être documenté. Une analyse de risques simplifiée (pas nécessairement selon une méthode formelle comme EBIOS Risk Manager) doit identifier les actifs critiques et les principaux risques pesant sur l'entreprise.

La sensibilisation des collaborateurs doit faire l'objet d'une session annuelle formelle, avec une trace documentaire (émargement, attestation de suivi e-learning ou compte-rendu de réunion).

Contrôle des accès Bronze : les exigences minimales

Le Bronze exige une politique de mots de passe documentée et appliquée techniquement : longueur minimale de 12 caractères, complexité (majuscules, minuscules, chiffres, caractères spéciaux), durée de validité maximale de 90 jours pour les comptes à privilèges. Les comptes génériques (admin, administrator, root) doivent être renommés ou désactivés.

Un inventaire des comptes actifs doit être tenu à jour. Les comptes des collaborateurs quittant l'entreprise doivent être désactivés dans les 24 heures suivant leur départ. Les comptes inactifs depuis plus de 90 jours doivent être revus et désactivés si non nécessaires.

Sécurité des systèmes Bronze : les fondamentaux

Un antivirus/EDR doit être déployé sur 100 % des postes de travail et des serveurs Windows, avec des mises à jour automatiques activées. Les mises à jour de sécurité du système

d'exploitation et des applications critiques (navigateurs, suites bureautiques) doivent être appliquées dans un délai maximum de 30 jours après leur publication.

Un pare-feu d'entreprise doit être en place, avec une règlementation des flux réseau documentée (pas uniquement le pare-feu Windows natif des postes). Les accès distants doivent passer par un VPN chiffré.

Protection des données Bronze

Le chiffrement des disques durs des postes nomades (ordinateurs portables) est obligatoire au Bronze. Les sauvegardes des données critiques doivent être réalisées selon la règle 3-2-1 (3 copies, sur 2 supports différents, dont 1 hors site), avec des tests de restauration au moins deux fois par an.

Erreurs courantes au niveau Bronze

Les non-conformités les plus fréquentes lors des audits Bronze sont : une politique de sécurité signée mais jamais communiquée aux collaborateurs, des mises à jour non appliquées sur des serveurs "oubliés" (imprimantes multifonctions, serveurs de fichiers anciens), l'absence de chiffrement sur les postes nomades, et des comptes d'anciens collaborateurs toujours actifs. Pensez à passer en revue l'annuaire Active Directory et à documenter votre processus de départ collaborateurs avant l'audit.

Niveau Silver — Parcours détaillé (120 contrôles, 6-8 mois)

Gestion avancée des identités — Les contrôles Silver

Le niveau Silver impose l'authentification multi-facteurs (MFA) pour tous les accès distants (VPN, webmail, portails partenaires) et pour tous les comptes administrateurs des systèmes critiques. La MFA ne peut pas être contournée par les utilisateurs ou désactivée sans validation du référent sécurité. La gestion des identités doit être centralisée (Active Directory, LDAP ou

solution équivalente), avec des processus documentés de création, modification et suppression de comptes.

Une revue trimestrielle des droits d'accès est obligatoire, avec un processus formel de validation par les responsables métier des accès accordés à leurs collaborateurs. Les droits d'accès doivent respecter le principe du moindre privilège : un collaborateur ne doit avoir accès qu'aux ressources nécessaires à ses fonctions.

Détection et réponse aux incidents — Silver

Le Silver exige la mise en place d'une capacité de détection centralisée. Cela peut prendre la forme d'un SIEM (Security Information and Event Management) interne ou externalisé, ou d'une solution de type MDR (Managed Detection and Response) proposée par un MSSP. Les logs des systèmes critiques (Active Directory, pare-feu, VPN, serveurs de fichiers) doivent être collectés et conservés pendant au moins 12 mois.

Des cas d'usage de détection adaptés au contexte de l'entreprise doivent être définis et implémentés : connexion en dehors des horaires de travail, tentatives d'authentification échouées répétées, transferts de volumes importants de données vers l'extérieur. Un processus de réponse aux incidents doit être documenté, incluant les rôles, les procédures d'escalade et les modalités de notification au GIFAS en cas d'incident majeur.

Sécurité des développements — Silver (si applicable)

Pour les entreprises qui développent des logiciels embarqués, des outils de gestion de production ou des applications internes, le Silver impose un cycle de développement sécurisé (SDLC). Cela inclut des revues de code sécurité, des tests de sécurité (analyse statique, tests de pénétration des applications) et une gestion des composants open-source (inventaire SBOM, vérification des vulnérabilités connues). Si votre entreprise n'effectue aucun développement logiciel, les contrôles de ce sous-domaine ne s'appliquent pas.

Erreurs courantes au niveau Silver

Les non-conformités Silver les plus fréquentes : une MFA déployée sur le VPN mais pas sur les webmails ou les portails partenaires (tous les accès distants doivent être couverts), des logs collectés mais jamais analysés (la collecte seule ne suffit pas, il faut démontrer une surveillance active), une revue des droits réalisée une fois mais pas trimestriellement (il faut des traces des quatre revues annuelles), et des procédures de réponse aux incidents écrites mais jamais testées en conditions réelles ou en exercice.

Niveau Gold — Parcours détaillé (180+ contrôles, 10-12 mois)

SOC et surveillance continue — Gold

Le Gold impose une capacité de surveillance de la sécurité 24h/24, 7j/7. Pour la plupart des PME et ETI, cela passe par l'externalisation à un SOC managé (Security Operations Center as a Service), avec un SLA de détection et de réponse à incident défini contractuellement. Les incidents critiques doivent pouvoir être détectés et traités en moins d'une heure. Des exercices de simulation d'attaque (red team ou purple team) doivent être réalisés annuellement.

Gestion avancée des tiers — Gold

Le Gold exige une évaluation cybersécurité formelle de tous les fournisseurs critiques (c'est-à-dire ceux ayant accès à vos systèmes d'information ou à vos données sensibles). Cette évaluation peut prendre la forme d'un questionnaire standardisé, d'un audit sur site ou de la vérification d'une certification équivalente. Des clauses contractuelles cybersécurité minimales doivent être intégrées dans tous les contrats avec ces fournisseurs, incluant le droit d'audit et l'obligation de notification en cas d'incident.

Intelligence des menaces — Gold

Le Gold requiert une capacité de veille sur les menaces ciblant spécifiquement le secteur aéronautique. Cela peut inclure l'abonnement à des flux CTI (Cyber Threat Intelligence) sectoriels, la participation aux groupes de partage d'information ISAC (Information Sharing and Analysis Center) du secteur, et la veille sur les vulnérabilités des équipements industriels et logiciels métier utilisés.

Préparation à l'audit GIFAS

Quelle que soit le niveau visé, la préparation à l'audit suit les mêmes bonnes pratiques :

4-6 semaines avant l'audit : Réalisez un pré-audit interne complet en vous basant sur la grille d'évaluation officielle GIFAS. Identifiez les points de non-conformité résiduels et évaluez leur criticité. Constituez le dossier documentaire (politiques, procédures, preuves de mise en œuvre).

2-3 semaines avant l'audit : Corrigez les non-conformités identifiées lors du pré-audit, notamment les points bloquants. Préparez les preuves techniques (captures d'écran de configuration, extraits de logs, listes d'utilisateurs, traces des revues des droits). Désignez les personnes qui seront interrogées lors de l'audit (direction, référent sécurité, administrateurs système).

Jour de l'audit : Préparez une salle dédiée avec accès aux systèmes et à la documentation. Soyez transparent sur les non-conformités connues et les plans de remédiation associés : les auditeurs GIFAS valorisent la maturité et la capacité d'amélioration continue, pas la perfection.

À RETENIR

À retenir

Bronze (~60 contrôles, 3-4 mois) se concentre sur les fondamentaux : politique de sécurité, gestion des accès basique, antivirus/EDR, mises à jour, sauvegarde. C'est un objectif atteignable pour toute PME avec les ressources adaptées.

Silver (~120 contrôles, 6-8 mois) ajoute la MFA pour tous les accès distants, la détection centralisée des incidents (SIEM/MDR), la revue trimestrielle des droits et le chiffrement renforcé. Il nécessite un audit par tiers accrédité.

Gold (180+ contrôles, 10-12 mois) exige une surveillance 24/7 (SOC externalisé ou interne), des exercices de simulation d'attaque annuels, la gestion formelle de la cybersécurité des tiers et une capacité CTI. C'est le niveau de référence pour les sous-traitants stratégiques.

Les non-conformités les plus fréquentes lors des audits sont : des politiques existantes mais non communiquées, des mises à jour manquantes sur des équipements "oubliés", l'absence de chiffrement sur les postes nomades, des comptes d'anciens collaborateurs actifs, et une MFA incomplète (certains accès distants non couverts).

Un pré-audit interne 4-6 semaines avant l'audit officiel est fortement recommandé pour identifier et corriger les derniers points de non-conformité sans surcoût.

FAQ — Certification AERO EXCELLENCE™ Bronze, Silver, Gold

Peut-on sauter le niveau Bronze pour aller directement au Silver ?

Techniquement, le référentiel ne l'interdit pas formellement, mais les contrôles Bronze sont des prérequis des contrôles Silver. Aucune entreprise ne peut raisonnablement satisfaire les contrôles Silver sans avoir d'abord maîtrisé les fondamentaux Bronze. En pratique, les auditeurs vérifieront que les contrôles Bronze sont bien satisfaits avant de valider le Silver. Il est donc recommandé de commencer par le Bronze, même si l'objectif à terme est le Silver.

Combien coûte l'audit GIFAS pour AERO EXCELLENCE™ V2 ?

Les coûts d'audit (hors mise en conformité) varient selon le niveau et la taille de l'entreprise. Pour une PME de 50-200 salariés : Bronze (vérification documentaire) entre 2 000 € et 5 000 €, Silver (audit sur site 1-2 jours) entre 5 000 € et 12 000 €, Gold (audit approfondi 2-4 jours) entre 10 000 € et 25 000 €. Ces tarifs sont ceux pratiqués par les organismes de vérification accrédités GIFAS et peuvent varier.

Que se passe-t-il si on échoue à l'audit AERO EXCELLENCE™ V2 ?

En cas de non-conformités mineures, un plan d'action correctif sous 3 mois est généralement accepté par l'organisme de vérification. Le label peut être attribué sous condition de la mise en œuvre du plan correctif, qui sera vérifiée lors d'un audit complémentaire. En cas de non-conformités majeures (absence d'antivirus, accès distants non sécurisés, politique de sécurité inexistante), l'audit est ajourné et l'entreprise doit engager une mise en conformité plus substantielle avant de représenter son dossier.

Peut-on faire certifier AERO EXCELLENCE™ V2 sur un périmètre restreint de l'entreprise ?

Oui, dans une certaine mesure. Le référentiel GIFAS permet de définir un périmètre de labellisation, par exemple limité à une entité ou à un site particulier. Cependant, les donneurs d'ordre peuvent exiger que le périmètre couvre au minimum toutes les activités en lien avec leurs commandes. Il est recommandé de clarifier avec chaque donneur d'ordre le périmètre attendu avant de définir le périmètre de labellisation.

Le label AERO EXCELLENCE™ V2 est-il reconnu par des donneurs d'ordre hors GIFAS ?

Le label AERO EXCELLENCE™ V2 est spécifique à la filière GIFAS. Cependant, sa structure est alignée sur des référentiels internationaux reconnus (ISO 27001, NIST CSF), ce qui peut lui valoir une reconnaissance partielle par des donneurs d'ordre étrangers ou hors filière. Dans le cadre de l'harmonisation européenne de la cybersécurité des supply chains, des discussions sont en cours pour que les certifications sectorielles nationales (AERO EXCELLENCE™ V2 en France, équivalents allemands, britanniques, etc.) soient mutuellement reconnues.

Outils et ressources pour faciliter votre parcours de certification

La préparation à la certification AERO EXCELLENCE™ V2 est facilitée par plusieurs outils et ressources mis à disposition par le GIFAS et ses partenaires. Les connaître et les utiliser dès le

début de votre démarche vous permettra d'économiser du temps et d'éviter les erreurs les plus courantes.

L'outil d'auto-diagnostic GIFAS

Le GIFAS met à disposition un outil d'auto-diagnostic en ligne accessible aux entreprises de la filière. Cet outil guide l'utilisateur à travers l'ensemble des contrôles du niveau visé (Bronze, Silver ou Gold), lui demandant pour chaque contrôle de s'auto-évaluer selon une échelle à quatre niveaux : Non initié, En cours de mise en place, Partiellement conforme, Conforme. À l'issue du questionnaire, l'outil génère un rapport de gaps priorisé qui identifie les non-conformités critiques, les non-conformités mineures et les points de vigilance. Ce rapport constitue la base du plan de remédiation.

Il est recommandé de réaliser l'auto-diagnostic avant même de décider du niveau à viser : les résultats permettent parfois de constater que le Silver est atteignable en quelques mois si des fondations solides existent déjà, ou au contraire que le Bronze lui-même nécessite un travail substantiel pour une entreprise peu mature en cybersécurité.

Les guides pratiques par domaine

Le GIFAS publie des guides pratiques par domaine de contrôle (gouvernance, accès, réseaux, etc.) qui explicitent le niveau d'exigence attendu pour chaque contrôle, fournissent des exemples de preuves acceptées lors de l'audit et proposent des recommandations d'implémentation adaptées aux PME. Ces guides sont indispensables pour éviter les malentendus lors de l'audit — car la formulation d'un contrôle peut laisser une marge d'interprétation significative.

Les formations GIFAS et partenaires

Plusieurs organismes de formation proposent des sessions dédiées à AERO EXCELLENCE™ V2 : sensibilisation des équipes dirigeantes (demi-journée), formation du référent sécurité (2 à 3 jours), et préparation à l'audit (1 journée). Ces formations sont éligibles au financement par les OPCO (Opérateurs de Compétences) dans le cadre du plan de développement des compétences.

Elles sont particulièrement utiles pour le référent sécurité de la PME, qui doit maîtriser le référentiel pour piloter efficacement la démarche de mise en conformité.

Maintien du label et amélioration continue

Obtenir le label AERO EXCELLENCE™ V2 n'est pas une fin en soi, mais le début d'une démarche d'amélioration continue. Le maintien du label sur les 3 années de validité suppose plusieurs obligations :

La surveillance annuelle

Chaque année, l'organisme de vérification réalise une surveillance documentaire : l'entreprise doit fournir des preuves que les contrôles continuent à être satisfaits. Cette surveillance couvre notamment la mise à jour de la politique de sécurité, la réalisation de la sensibilisation annuelle des collaborateurs, la revue des droits d'accès (trimestrielle pour le Silver), et la documentation des incidents éventuels survenus dans l'année avec les mesures correctives prises.

La gestion des évolutions du SI

Tout changement significatif du système d'information (migration vers un nouveau cloud, changement d'ERP, ouverture d'un nouveau site, fusion avec une autre entreprise) doit être documenté et évalué au regard des impacts sur les contrôles certifiés. Si une évolution réduit le niveau de conformité sur un contrôle, une mesure compensatoire doit être mise en place dans des délais définis.

La préparation du renouvellement

À 6 mois de l'échéance des 3 ans, il est recommandé d'engager la préparation du renouvellement. Le paysage des menaces et les exigences du référentiel ayant évolué, le renouvellement peut

apporter des nouvelles exigences à satisfaire. Cette préparation anticipée évite la pression d'un audit de renouvellement sur un délai trop court.

Pour vous accompagner dans l'obtention et le maintien de votre certification AERO EXCELLENCE™ V2, consultez notre offre dédiée sur notre page AERO EXCELLENCE™ et notre service d'accompagnement AirCyber. Les ressources officielles sont disponibles sur gifas.asso.fr et sur le portail cybersécurité national cyber.gouv.fr. L'ANSSI propose également des ressources complémentaires sur la sécurité des systèmes d'information industriels.

Questions fréquentes sur le financement et l'organisation de la démarche

Au-delà des questions techniques, les PME se posent souvent des questions pratiques sur le financement et l'organisation interne de la démarche de certification AERO EXCELLENCE™. Voici quelques réponses aux interrogations les plus fréquentes :

Qui doit piloter la démarche en interne ? Dans une PME sans RSSI dédié, le référent sécurité nommé pour le label peut être le DSI, le responsable qualité (déjà habitué aux démarches de certification ISO 9001 ou EN 9100), ou un manager polyvalent formé spécifiquement. L'essentiel est que ce référent ait le soutien explicite de la direction générale et un budget dédié. La direction générale doit signer la politique de sécurité et approuver les investissements, même si la mise en œuvre opérationnelle est déléguée.

Peut-on faire appel à un consultant externe comme référent sécurité ? Oui, et c'est même une pratique courante pour les PME de moins de 50 salariés. Un RSSI externalisé (vRSSI) peut piloter la démarche AERO EXCELLENCE™ V2, constituer le dossier documentaire, préparer et accompagner l'audit. Cette formule est généralement plus économique qu'un recrutement à temps plein. Consultez notre offre RSSI externalisé pour AERO EXCELLENCE™ et les ressources de l'ANSSI sur cyber.gouv.fr et du GIFAS.

Accompagnement AERO EXCELLENCE™ et AirCyber BoostAerospace

Nos consultants certifiés vous guident dans le parcours Bronze → Silver → Gold, en croisant les exigences GIFAS et AirCyber BoostAerospace pour maximiser la valeur de chaque démarche.

Demander un devis sous 48h →

Comparatif des trois niveaux de certification AERO EXCELLENCE™ (Bronze, Silver, Gold)

Domaine de contrôle	Bronze	Silver	Gold	Écart d'audit fréquent
Gouvernance et politique de sécurité	Politique SSI signée par la direction	Comité de pilotage et revue annuelle formalisée	Gouvernance intégrée au SMSI, indicateurs suivis en CODIR	Politique existante mais jamais revue ni diffusée
Gestion des risques	Inventaire des actifs critiques	Analyse de risques documentée et plan de traitement	Méthode formalisée (EBIOS RM) et réévaluation périodique	Analyse de risques figée, non mise à jour après changements
Contrôle d'accès et identités	Comptes nominatifs, MFA sur les accès distants	Revue périodique des droits, gestion des comptes à privilèges	Tiering Active Directory, PAM et journalisation des privilèges	Comptes de départs non désactivés, aucune preuve de revue
Sécurité des systèmes et des réseaux	Antivirus, pare-feu, correctifs appliqués	Segmentation réseau, durcissement des configurations	EDR, supervision continue et tests d'intrusion réguliers	Correctifs déployés sans politique de patch management écrite
Sauvegardes et continuité d'activité	Sauvegardes régulières, copie hors ligne	PCA/PRA documenté, RTO et RPO définis	Tests de restauration annuels tracés et exercices de crise	Sauvegardes fonctionnelles mais restaurations jamais testées
Gestion des incidents	Point de contact identifié et procédure d'alerte	Processus de qualification, journalisation centralisée	Cellule de crise, SOC/SIEM et retours d'expérience formalisés	Incidents traités mais aucun registre ni post-mortem
Sécurité de la chaîne d'approvisionnement	Liste des fournisseurs critiques	Clauses de sécurité contractuelles, questionnaires fournisseurs	Évaluation et audit des sous-traitants de rang 2	Exigences transmises oralement, sans clause contractuelle
Sensibilisation et ressources humaines	Sensibilisation à l'arrivée, charte informatique	Plan de sensibilisation annuel avec émargement	Campagnes de phishing simulé et formations par profil	Sessions réalisées sans preuve de participation conservée

Conclusion

La conformité réglementaire n'est pas une destination mais un état à maintenir. Chaque évolution du SI, chaque nouveau fournisseur peut modifier le périmètre. Documentation, audits réguliers et formation des équipes en sont les piliers.

Votre organisation est-elle soumise à NIS 2, ISO 27001 ou DORA ?

Évaluer votre conformité NIS 2 ou contactez-nous directement.