RMC DGA : Le Référentiel de Maturité Cyber pour les Fournisseurs Défense

Le Référentiel de Maturité Cyber de la Direction Générale de l'Armement — le RMC DGA — constitue aujourd'hui le cadre de référence incontournable pour toute entreprise souhaitant accéder aux marchés de la défense française. Publié par la DGA (Direction Générale de l'Armement) dans le cadre de la politique de sécurité des systèmes d'information du ministère des Armées, il définit un socle minimal d'exigences cybersécurité que les fournisseurs de la Base Industrielle et Technologique de Défense (BITD) doivent satisfaire. Face à la multiplication des cyberattaques ciblant la chaîne d'approvisionnement industrielle de défense — illustrée notamment par les incidents touchant des sous-traitants européens entre 2022 et 2025 — la DGA a formalisé ce référentiel pour structurer le niveau de maturité cyber de ses partenaires industriels. Ce guide complet vous explique l'historique du RMC DGA, ses objectifs, l'architecture en trois niveaux, les 32 mesures du niveau Fondamental, son articulation avec le SSID et ISO 27001, et le processus d'évaluation concret pour les PME de la BITD.

Historique et contexte du RMC DGA

La genèse du RMC DGA s'inscrit dans une prise de conscience progressive du ministère des Armées quant à la vulnérabilité de sa chaîne de sous-traitance. Dès 2017, plusieurs incidents impliquant des fournisseurs de rang 2 et 3 avaient mis en évidence des lacunes significatives en matière de protection des informations sensibles. La fuite de données techniques relatives à des équipements embarqués, survenue dans une PME sous-traitante d'un maître d'œuvre principal, avait sonné l'alarme au plus haut niveau de la DGA.

En réponse, la DGA a engagé entre 2019 et 2022 un travail de formalisation d'un référentiel adapté aux réalités des industriels de la défense, en particulier les PME et ETI qui représentent plus de 4 000 entreprises dans la BITD française. Le RMC DGA s'inspire des travaux menés aux

États-Unis avec le CMMC (Cybersecurity Maturity Model Certification) tout en l'adaptant au contexte réglementaire français, notamment aux exigences issues de l'Instruction Générale Interministérielle n°1300 (IGI 1300) sur la protection du secret de la défense nationale.

Le référentiel a été progressivement intégré dans les clauses contractuelles des marchés DGA à partir de 2023, avec une montée en puissance accélérée dans le cadre de la Loi de Programmation Militaire (LPM) 2024-2030, qui prévoit une enveloppe de 413 milliards d'euros pour les armées françaises. Cette dynamique budgétaire s'accompagne d'exigences de sécurité renforcées pour l'ensemble de la chaîne d'approvisionnement.

Les objectifs du RMC DGA

Le RMC DGA poursuit trois objectifs fondamentaux complémentaires, qui structurent l'ensemble de son architecture normative.

Protéger les informations sensibles tout au long de la chaîne

Le premier objectif est la protection des informations non classifiées à diffusion restreinte (DR) et des informations classifiées de défense circulant dans la chaîne industrielle. Même un fournisseur de rang 3 — qui ne manipule a priori que des spécifications techniques partielles — peut détenir des fragments d'information dont la combinaison constitue un risque pour la sécurité nationale. Le RMC DGA impose donc un socle minimal de protection indépendamment du rang du fournisseur dans la chaîne.

Harmoniser le niveau de sécurité entre fournisseurs

Le deuxième objectif est la mise en place d'un langage commun et d'un niveau de sécurité homogène entre les différents acteurs de la BITD. Avant le RMC DGA, chaque maître d'œuvre (Thales, Airbus Defence, Naval Group, Safran, MBDA, etc.) imposait ses propres questionnaires et exigences à ses sous-traitants, créant une multiplication des audits et une confusion normative préjudiciable aux PME. Le RMC DGA standardise ces exigences.

Permettre une évaluation objective et progressive

Le troisième objectif est de fournir un cadre d'évaluation objectif permettant aux fournisseurs de démontrer leur niveau de maturité cyber à leur donneur d'ordres, tout en leur offrant une trajectoire d'amélioration progressive et réaliste. L'architecture en trois niveaux répond précisément à ce besoin de gradation.

Les trois niveaux du RMC DGA

Le RMC DGA s'organise en trois niveaux de maturité croissants, chacun correspondant à un profil de risque et un type de fournisseur spécifiques.

Niveau 1 — Fondamental

Le niveau Fondamental constitue le socle minimal exigé pour tout fournisseur ayant accès à des informations sensibles non classifiées dans le cadre de marchés DGA. Il comprend 32 mesures de sécurité organisées en 8 domaines : gouvernance, gestion des accès, protection des postes de travail, sécurité réseau, gestion des correctifs, sauvegarde et continuité, sensibilisation du personnel, et gestion des incidents. Ce niveau est accessible aux PME disposant d'une DSI interne légère ou faisant appel à un prestataire MSSP. Le délai moyen de mise en conformité constaté est de 4 à 9 mois selon le niveau de maturité initial.

Niveau 2 — Intermédiaire

Le niveau Intermédiaire s'adresse aux fournisseurs manipulant des volumes significatifs d'informations sensibles ou intervenant sur des programmes d'armement majeurs. Il élargit le périmètre des 32 mesures Fondamentales avec des exigences supplémentaires en matière de détection d'incidents (SOC), de tests d'intrusion réguliers, de gestion avancée des identités (MFA pour tous les accès systèmes), et d'architecture de sécurité documentée. Les entreprises de niveau

Intermédiaire doivent généralement s'appuyer sur un RSSI à temps plein et des outils de supervision (SIEM, EDR).

Niveau 3 — Avancé

Le niveau Avancé est réservé aux maîtres d'œuvre industriels et aux fournisseurs critiques manipulant des informations classifiées ou participant à des programmes de souveraineté nationale. Il intègre des exigences de threat intelligence, de red team régulier, de cloisonnement réseau avancé (zones sécurisées, salles blanches numériques) et d'audit externe par un tiers qualifié. Peu d'entreprises atteignent ce niveau dans la BITD, et celles qui y prétendent sont généralement déjà certifiées ISO 27001 ou qualifiées ANSSI.

Les 32 mesures du niveau Fondamental

Le cœur opérationnel du RMC DGA Fondamental réside dans ses 32 mesures concrètes, réparties sur 8 domaines de sécurité. Ces mesures sont toutes obligatoires — il n'existe pas de mesure optionnelle au niveau Fondamental.

Domaine 1 : Gouvernance cyber (4 mesures)

Ce domaine impose la désignation formelle d'un référent cybersécurité (qui peut être externe), la rédaction d'une politique de sécurité des systèmes d'information (PSSI) approuvée par la direction, la réalisation d'un inventaire des actifs informatiques couvrant au minimum les serveurs, postes de travail, équipements réseau et données sensibles, et la mise en place d'un processus de révision annuelle de la PSSI.

Domaine 2 : Gestion des accès (5 mesures)

Les cinq mesures de ce domaine couvrent : la politique de mots de passe robuste (longueur minimale 12 caractères, complexité, sans réutilisation sur 12 itérations), le déploiement de

l'authentification à double facteur (MFA) pour tous les accès distants et les comptes administrateurs, la gestion des comptes privilégiés avec traçabilité, la révocation immédiate des accès lors des départs, et l'interdiction des comptes génériques ou partagés.

Domaine 3 : Protection des postes (4 mesures)

Ce domaine exige le déploiement d'un antivirus/EDR sur 100 % du parc, le chiffrement des disques durs (BitLocker ou équivalent), la gestion des supports amovibles (interdiction ou contrôle par liste blanche), et l'application d'une politique de verrouillage automatique après inactivité.

Domaine 4 : Sécurité réseau (5 mesures)

Les exigences réseau portent sur la segmentation entre réseau bureautique et systèmes sensibles, le filtrage des flux entrants et sortants par pare-feu correctement configuré, l'interdiction des protocoles réseaux non chiffrés pour les accès aux ressources sensibles (exit Telnet, FTP non sécurisé), la sécurisation des accès Wi-Fi (WPA2/WPA3, séparation réseau invités), et la journalisation des connexions réseau avec conservation 90 jours minimum.

Domaine 5 : Gestion des correctifs (3 mesures)

Ce domaine impose un processus formel de veille sur les vulnérabilités (CVE critiques et élevées), l'application des correctifs de sécurité critiques sous 30 jours, et la mise à jour ou le remplacement des systèmes en fin de support (EOL).

Domaine 6 : Sauvegarde et continuité (4 mesures)

La politique de sauvegarde doit couvrir l'ensemble des données sensibles avec une fréquence au moins quotidienne, un stockage hors ligne ou hors site (règle 3-2-1), des tests de restauration documentés mensuellement, et un plan de continuité d'activité (PCA) ou plan de reprise d'activité (PRA) formalisé, même minimal.

Domaine 7 : Sensibilisation (3 mesures)

Le RMC DGA exige a minima une sensibilisation annuelle de l'ensemble du personnel aux risques cyber (phishing, mots de passe, ingénierie sociale), une procédure documentée pour signaler les incidents suspects, et une sensibilisation spécifique des personnels accédant aux informations défense les plus sensibles.

Domaine 8 : Gestion des incidents (4 mesures)

Ce dernier domaine impose la mise en place d'une procédure de réponse aux incidents formalisée, la désignation d'un point de contact opérationnel joignable en cas d'incident, la capacité à notifier la DGA et/ou l'ANSSI en cas d'incident touchant des informations défense dans un délai de 72 heures, et la conservation des journaux d'audit pendant 12 mois minimum.

Articulation avec le SSID

Le RMC DGA s'articule étroitement avec le référentiel SSID (Sécurité des Systèmes d'Information Défense), qui constitue le cadre normatif global du ministère des Armées pour la protection des systèmes d'information manipulant des informations classifiées. Le SSID est défini par l'Instruction Interministérielle n°901 (II 901) et s'applique aux systèmes classifiés Confidentiel Défense et Secret Défense.

La relation entre RMC DGA et SSID est de complémentarité hiérarchique : le RMC DGA Fondamental couvre le périmètre des systèmes non classifiés ou à diffusion restreinte, tandis que le SSID prend le relais pour les systèmes classifiés. Un fournisseur qui développe à la fois des composants non classifiés et des modules classifiés doit se conformer aux deux référentiels, le SSID étant plus exigeant et imposant des procédures d'homologation formelles.

En pratique, une entreprise conforme au RMC DGA niveau Intermédiaire ou Avancé dispose d'une base solide pour engager une démarche SSID, les contrôles des deux référentiels se recoupant significativement sur les aspects gouvernance, gestion des accès, et journalisation.

RMC DGA vs ISO 27001 : différences essentielles

La question la plus fréquente des industriels BITD concerne la relation entre RMC DGA et ISO 27001. Ces deux référentiels sont complémentaires mais non équivalents.

L'ISO 27001 est une norme internationale de management de la sécurité de l'information, centrée sur la mise en place d'un Système de Management de la Sécurité de l'Information (SMSI) et basée sur une approche par les risques. Elle ne prescrit pas de mesures techniques spécifiques mais exige une démonstration de la pertinence et de l'efficacité des contrôles choisis par l'organisation. Sa certification est délivrée par des organismes accrédités (Bureau Veritas, LRQA, etc.) après audit tierce partie.

Le RMC DGA Fondamental est au contraire prescriptif : les 32 mesures sont imposées indépendamment d'une analyse de risque propre à l'entreprise. C'est une approche de conformité binaire (conforme / non conforme sur chaque mesure) plutôt qu'une approche de management du risque. La reconnaissance contractuelle est opérée directement par la DGA ou les maîtres d'œuvre, sans certification formelle par tierce partie pour le niveau Fondamental.

Une entreprise certifiée ISO 27001 ne peut pas prétendre automatiquement au RMC DGA Fondamental : elle doit démontrer que son SMSI couvre effectivement les 32 mesures prescrites. Inversement, la conformité RMC DGA Fondamental constitue une bonne préparation à l'ISO 27001, qui exige cependant un niveau de formalisation et de revue de direction supplémentaire.

Processus d'évaluation : comment ça se passe concrètement

L'évaluation RMC DGA ne repose pas à ce jour sur une certification formelle délivrée par un organisme tiers pour le niveau Fondamental. Elle se traduit par une auto-déclaration de conformité, accompagnée d'un dossier de preuves, transmis au donneur d'ordres (maître d'œuvre ou DGA directement).

Le processus typique comprend quatre étapes : un diagnostic initial permettant d'identifier les écarts par rapport aux 32 mesures, un plan d'action priorisé avec jalons de mise en conformité, la

constitution d'un dossier de preuves documentaires (captures d'écran, procédures, journaux, rapports d'audit), et une revue par le donneur d'ordres qui peut inclure un entretien ou un audit documentaire partiel.

Pour les PME de la BITD, le recours à un prestataire spécialisé comme un consultant cybersécurité PME ou un RSSI externalisé est fortement recommandé pour structurer cette démarche dans des délais et budgets maîtrisés. Voir aussi notre guide pas-à-pas conformité RMC DGA pour PME.

Cas pratiques PME BITD

Cas 1 : PME d'électronique embarquée (50 salariés)

Une PME normande de 50 salariés, sous-traitante de rang 2 d'un groupement pour un programme de véhicule de combat, s'est vue imposer la conformité RMC DGA Fondamental lors du renouvellement de son contrat en 2024. Après un diagnostic révélant 14 écarts sur les 32 mesures (principalement sur la gestion des correctifs, le MFA, et l'absence de PCA), l'entreprise a engagé une démarche de 7 mois avec un RSSI externalisé. Le coût total de mise en conformité a été de l'ordre de 45 000 euros, dont 60 % en solutions techniques (EDR, sauvegarde, firewall nouvelle génération) et 40 % en accompagnement conseil.

Cas 2 : ETI de maintenance aéronautique militaire (280 salariés)

Une ETI de maintenance aéronautique militaire, déjà certifiée ISO 9001 et engagée dans une démarche ISO 27001, a pu valoriser ses travaux existants pour réduire le périmètre d'effort RMC DGA. Les 8 domaines présentaient des gaps principalement sur la journalisation des accès réseau et la gestion des supports amovibles. La mise en conformité complémentaire a nécessité 3 mois et un investissement inférieur à 15 000 euros, la structure étant déjà bien organisée sur les volets gouvernance et sensibilisation.

Les enjeux stratégiques du RMC DGA pour la souveraineté nationale

La mise en place du RMC DGA s'inscrit dans une vision stratégique plus large portée par le ministère des Armées : reconquérir la maîtrise de la chaîne d'approvisionnement industrielle de défense face aux menaces d'espionnage économique et d'intrusions étatiques ciblées. Les acteurs de la menace les plus actifs contre la BITD française sont bien identifiés : des groupes APT (Advanced Persistent Threat) agissant pour le compte d'États étrangers cherchant à obtenir des informations sur les capacités militaires françaises, les procédés de fabrication d'équipements sensibles, ou les failles exploitables dans les systèmes en service. Les campagnes d'espionnage industriel ciblant des sous-traitants de la défense européens sont en augmentation constante depuis 2020, avec une accélération notable depuis le retour de la guerre conventionnelle en Europe. Le RMC DGA répond à cette menace en créant un socle de protection homogène qui complique significativement le travail des attaquants ciblant la chaîne de sous-traitance comme vecteur d'accès indirect aux systèmes militaires.

Le rôle des maîtres d'œuvre industriels dans le déploiement du RMC DGA

Les grands maîtres d'œuvre de la BITD — Thales, Airbus Defence & Space, Naval Group, Safran, MBDA, Dassault Aviation — jouent un rôle central dans le déploiement du RMC DGA au sein de leur chaîne de sous-traitance. Chacun a développé ses propres processus d'évaluation et d'accompagnement des fournisseurs, généralement inspirés du cadre DGA mais enrichis de leurs propres exigences sectorielles. Thales, par exemple, a mis en place un programme "Cyber Supply Chain" qui impose à ses fournisseurs un questionnaire d'auto-évaluation aligné sur le RMC DGA et propose des ressources d'accompagnement pour les PME en difficulté. Naval Group a déployé un dispositif similaire avec des audits documentaires ciblés pour ses sous-traitants travaillant sur des programmes de bâtiments de combat. Ces initiatives des maîtres d'œuvre créent un effet de cascade positif : une PME qui satisfait aux exigences cybersécurité d'un grand industriel de la défense dispose généralement d'une conformité RMC DGA solide. Elles peuvent aussi générer une certaine hétérogénéité dans les exigences, chaque maître d'œuvre ajoutant ses propres couches au-dessus du socle DGA.

Perspectives d'évolution du RMC DGA 2026-2030

Le RMC DGA n'est pas figé. Plusieurs évolutions sont attendues dans la période 2026-2030, en phase avec la montée en puissance de la LPM et les enseignements tirés des premiers déploiements du référentiel. La principale évolution anticipée est l'introduction d'une certification tierce partie obligatoire pour le niveau Intermédiaire, s'inspirant du modèle CMMC américain. Cette évolution permettrait de renforcer la crédibilité des déclarations de conformité et de faciliter la reconnaissance mutuelle dans le cadre des coopérations de défense européennes (OCCAR, EDIDP, FED). Une deuxième évolution attendue concerne l'extension du RMC DGA aux fournisseurs de services numériques (cloud, SaaS, infogérance) au service d'industriels de la défense, un vide actuellement partiellement comblé par les exigences contractuelles NIS 2. Enfin, l'harmonisation croissante avec les référentiels cybersécurité des partenaires européens (CMMC aux États-Unis, BSI IT-Grundschutz en Allemagne, NCSC Cyber Essentials au Royaume-Uni) devrait progressivement réduire la complexité pour les industriels travaillant sur des programmes multinationaux. Pour suivre ces évolutions, consulter régulièrement les publications de la DGA et de l'ANSSI est indispensable. Notre équipe publie également des mises à jour régulières dans nos articles conformité.

À RETENIR

Ce qu'il faut retenir

Le RMC DGA est le référentiel de maturité cyber de la DGA, obligatoire pour les fournisseurs BITD accédant à des informations sensibles défense

Il comprend 3 niveaux (Fondamental, Intermédiaire, Avancé) et 32 mesures prescriptives au niveau Fondamental, réparties sur 8 domaines

Le niveau Fondamental est distinct de l'ISO 27001 : il est prescriptif et non basé sur une analyse de risque propre à l'entreprise

> Il s'articule avec le SSID pour les systèmes d'information classifiés, le RMC DGA couvrant les systèmes non classifiés ou à diffusion restreinte
>
> La mise en conformité Fondamentale est accessible aux PME en 4 à 9 mois avec l'appui d'un prestataire spécialisé

FAQ RMC DGA

Le RMC DGA est-il obligatoire pour tous les fournisseurs DGA ?

Non, le RMC DGA s'applique aux fournisseurs ayant accès à des informations sensibles dans le cadre de marchés DGA. Les fournisseurs ne manipulant que des composants standardisés sans accès aux données du programme peuvent ne pas être concernés. L'applicabilité est précisée dans les clauses contractuelles de chaque marché.

Existe-t-il une certification officielle RMC DGA délivrée par un organisme tiers ?

Au niveau Fondamental, le RMC DGA fonctionne sur la base d'une auto-déclaration de conformité avec dossier de preuves. Il n'existe pas à ce jour de certification formelle délivrée par un organisme tiers accrédité, contrairement à l'ISO 27001. Des évolutions vers un modèle de certification tierce partie sont envisagées pour les niveaux Intermédiaire et Avancé.

Le RMC DGA remplace-t-il l'ISO 27001 pour les fournisseurs défense ?

Non. Les deux référentiels sont complémentaires. Une certification ISO 27001 ne suffit pas à démontrer la conformité RMC DGA, car les 32 mesures Fondamentales sont prescriptives et peuvent ne pas être couvertes par le périmètre du SMSI ISO 27001. Certains maîtres d'œuvre exigent les deux certifications pour leurs fournisseurs critiques.

Combien de temps faut-il pour atteindre le niveau Fondamental ?

Le délai moyen constaté est de 4 à 9 mois selon le niveau de maturité initial de l'entreprise. Une PME partant de zéro peut raisonnablement viser 6 à 8 mois. Une structure déjà bien organisée sur la cybersécurité (ISO 27001 en cours, PSSI existante) peut atteindre le niveau Fondamental en 3 à 4 mois.

Quelles ressources officielles consulter sur le RMC DGA ?

Les informations officielles sur le RMC DGA sont publiées sur le site de la DGA (defense.gouv.fr/dga) et relayées par le GIP ACYMA (cyber.gouv.fr). L'ANSSI publie également des guides techniques applicables aux mesures techniques du référentiel.

