BULLETIN OFFICIEL DES ARMEES

Edition Chronologique n°51 du 9 décembre 2011

PARTIE PERMANENTE
Administration Centrale

Texte n°1

INSTRUCTION N° 2007/DEF/DGSIC
relative au pilotage d'un système d'information outillant les processus de fonctionnement du ministère, de la conception au retrait de service.

Du *30 septembre 2011*

DIRECTION GÉNÉRALE DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION.

INSTRUCTION N° 2007/DEF/DGSIC relative au pilotage d'un système d'information outillant les processus de fonctionnement du ministère, de la conception au retrait de service.

Du 30 septembre 2011

NOR D E F E 1 1 5 1 8 6 4 J

Pièce(s) Jointe(s) :

Six annexes.

Classement dans l'édition méthodique : BOEM 160.1

Référence de publication : BOC N°51 du 9 décembre 2011, texte 1.

SOMMAIRE

3.2. En conduite de projet (jusqu’au stade d’utilisation).

3.2.1. Responsable fonctionnel du projet.

3.2.2. Responsable de conduite de projet

3.2.3. Responsable fonctionnel d'ensemble, responsable de conduite de projet d'ensemble.

3.2.4. Responsable de réalisation du projet.

3.2.5. Conduite de projet intégrée - en réseau ou en équipe dédiée.

3.2.6. Comité des utilisateurs.

3.2.7. Responsabilité de réalisation.

3.2.8. Responsabilité de déploiement.

3.3. Au stade d'utilisation.

3.3.1. Responsable fonctionnel du système.

3.3.2. Responsable technique de système.

3.3.3. Responsable de sécurité des systèmes d'information aval.

3.3.4. Maintien en condition opérationnelle.

3.3.5. Fonction d'exploitation.

3.3.6. Fonction de soutien aux utilisateurs.

3.4. Instances de décision et d’examen.

3.4.1. Comité de direction du projet puis du système en exploitation.

3.4.2. Comité de pilotage du projet.

3.4.3. Comité de gestion de la configuration du système.

3.4.4. Commission d'homologation du projet puis du système en exploitation.

3.4.5. Groupe de travail d'examen de projet - groupe d'instruction des systèmes.

3.5. Opérateur.

3.6. Sécurité des systèmes d'information.

3.6.1. Autorité qualifiée.

3.6.2. Autorité d'homologation.

3.7. Contrôle financier.

3.7.1. Responsable de budget opérationnel de programme.

ANNEXE(S)

1. OBJECTIFS ET DOMAINE D'APPLICATION.

Cette instruction définit les rôles et responsabilités génériques à exercer et les activités à conduire pour concevoir, réaliser, et utiliser un système d'information (SI), sans préjuger de leur distribution dans l'organisation du ministère.

Elle intervient en aval de l'élaboration du besoin (définition ou évolution de l'organisation et des processus à outiller), qui relève d'une autre instruction.

Cette instruction précise l'enchaînement des activités nécessaires et définit le processus de conduite d'un SI pour chaque stade :

- conception, en passant par le stade d'études, jusqu'à la fin du stade de développement ;

- évolutions majeures (évolutions du périmètre fonctionnel, refonte technique, etc.) traitées comme de nouveaux projets, en suivant cette instruction ;

- utilisation et retrait de service. Dans ces stades, l'organisation en « mode projet » est remplacée par une organisation en «mode conduite de système », les acteurs pouvant rester les mêmes. Pendant le stade d'utilisation, une version N peut être en service, tandis qu'une version N+1 (évolution majeure) est en projet (études et/ou développement).

Elle indique, pour chaque stade, les activités à conduire, les résultats attendus, les contrôles à effectuer. Certaines activités peuvent être regroupées et/ou développées en fonction de la complexité du projet.

Elle souligne la nécessité d'une collaboration et d'une concertation étroite pendant toute la durée du projet, entre les différents acteurs internes ou externes au ministère. Cette concertation et ce travail commun s'exercent en particulier dans le cadre des instances et de l'équipe intégrée mise en place pour le projet.

Un plan de management doit être établi et doit préciser l'attribution des responsabilités, l'organisation nécessaire et suffisante mise en place (selon la complexité du projet), les éventuels compléments ou aménagements dans l'enchaînement des activités, et enfin les documents (issus de l'annexe III.) qui devront être formalisés en plus de ceux obligatoires déjà prévus (cf. chapitre IV.).

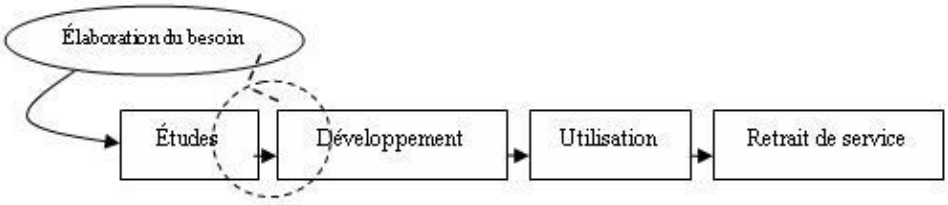
Cette instruction s'applique aux SI outillant les processus de fonctionnement du ministère : SI d'administration et gestion (SIAG), SI opérationnels (SIO) non érigés en opération d'armement (1), et ceux des systèmes d'information scientifiques et techniques (SIST) pour lesquels la direction générale de l'armement (DGA) le décide.

2. STADES ET ACTIVITÉS PRINCIPALES.

L'élaboration du besoin comprend la définition ou la révision de l'organisation du travail et des processus à outiller, sous la responsabilité des organismes métiers. Elle fait l'objet d'une instruction séparée.

L'étude du besoin exprimé, la conception, la réalisation et le déploiement d'une solution, l'utilisation dans les conditions définies puis le retrait de service d'un système forment une suite de grandes activités, où « clients » et « fournisseurs » restent en liaison pour optimiser la solution élaborée.

L'analyse détaillée des activités à conduire est en annexe III.



Nota. Les versions sucessives d'un SI peuvent coexister, en général à des stades différents de leur cycle de vie.

2.1. **L'étude du besoin.**

*2.1.1. **Analyse du besoin.***

Outre les spécifications fonctionnelles, l'expression de besoin doit comprendre l'identification de toutes les contraintes d'environnement et d'utilisation ainsi que les objectifs de SSI. Ces éléments sont rassemblés dans un dossier d'expression du besoin.

Dans des cas complexes : une ou plusieurs itérations peuvent être nécessaires entre cette phase et la phase de conception.

*2.1.2. **Mise en place de l'ensemble des moyens nécessaires et suffisants.***

Mise en place des compétences ou équipes de conduite de projet, de réalisation et hébergement du SI au niveau de sécurité requis.

Les moyens financiers sont à estimer et prévoir, ainsi que le mode d'acquisition et la couverture contractuelle nécessaire.

L'organisation de ces moyens et leur mise en œuvre sont détaillées dans un plan de management.

2.2. **La conception, la réalisation et le déploiement d'un système.**

2.2.1. ***Conception et réalisation du système.***

Ces activités doivent conduire à la fourniture : d'un système conforme, des vérifications de cette conformité, et de l'ensemble des documentations techniques et fonctionnelles liées.

2.2.2. ***Intégration et déploiement du système.***

Ces activités doivent conduire à la mise en service dans les meilleures conditions d'un système accessible à l'ensemble de ses utilisateurs.

La conduite du changement fait partie intégrante de cette phase.

2.3. **L'utilisation.**

Ces activités comprennent l'exploitation du système dans les conditions d'utilisation et de sécurité prévues, ainsi que la spécification et la réalisation des corrections et évolutions mineures et la préparation du retrait de service (le maintien en condition opérationnelle et de sécurité).

Les évolutions majeures doivent être conduites comme un nouveau projet, à l'issue d'une phase d'élaboration du besoin.

2.4. **Le retrait de service.**

Cette action doit s'accompagner d'un archivage, d'une reprise par un nouveau système, et/ou d'une destruction des données.

Le retrait de service est prononcé par le responsable de zone fonctionnelle sur demande des l'autorités utilisatrices. Elles définissent le sort qui doit être reservé aux données génrées par le SI depuis le début de son utilisation.

3. RÔLES ET RESPONSABILITÉS.

Ne sont traités ici que les rôles et responsabilités directement liés à la conduite de projet. La gouvernance générale des SI du ministère est décrite par ailleurs.

3.1. **Gouvernance générale.**

3.1.1. ***Autorité « cliente ».***

L'autorité « cliente » (AC) est l'autorité responsable de l'activité métier ou transverse à instrumenter ou à automatiser et, le cas échéant, responsable du processus concerné. Elle définit pour le compte de tous les futurs utilisateurs le besoin fonctionnel, le périmètre du projet et sa date de mise en service opérationnel (MSO) souhaitée. Elle définit de manière globale, les conditions de mise en œuvre du SI par les utilisateurs et les objectifs de sécurité (modes de travail, processus, articulation avec d'autres métiers, etc.).

L'AC préside le comité directeur (CODIR) du projet.

Dès la phase d'expression du besoin, l'AC désigne un responsable fonctionnel (RF) qui portera le besoin pendant toute la vie du SI de sa conception à son retrait de service.

Le terme d'AC dans la suite du texte représente soit une autorité ou son représentant, soit sa responsabilité.

3.1.2. ***Autorités utilisatrices.***

Les autorités « utilisatrices » (AU) précisent à l'AC et au RF, les conditions de mise en œuvre du SI et les objectifs de sécurité (modes de travail, processus, articulation avec d'autres métiers, etc.) de leur responsabilité.

Les AU sont présentes ou représentées au CODIR du projet.

Les AU désignent des représentants au comité des utilisateurs lorsque celui-ci est créé.

Le terme d'AU dans la suite du texte représente soit une autorité ou son représentant, soit sa responsabilité.

3.1.3. ***Responsable de secteur fonctionnel.***

Les responsables de zone fonctionnelle (RZF) et les responsables de quartier fonctionnel (RQF) sont chargés d'assurer la cohérence et l'alignement stratégique des systèmes d'information et de communication (SIC) dans le secteur fonctionnel, du plan d'occupation des sols du ministère (POS) qui leur est confié.

Les RZF et les RQF rédigent et entretiennent les schémas directeurs SIC (volets opérationnels) de leur secteur fonctionnel (cf. définition en annexe I.). Ils optimisent le fonctionnement d'ensemble des SIC de leur zone et en organisent la mise en œuvre. Ils sont en particulier responsables de l'optimisation des processus et de la réduction du nombre d'applications par fonction, en liaison avec les autorités responsables de l'organisation et de l'emploi des SI. Ils se prononcent sur l'opportunité de lancer ou non le projet, sur les modalités de retrait des applications et sur les interfaces avec les SI des autres secteurs fonctionnels.

3.1.4. ***Direction générale des systèmes d'information et de communication.***

La direction générale des systèmes d'information et de communication (DGSIC) oriente, anime et coordonne les actions du ministère visant à améliorer la qualité, l'efficacité, l'efficience et la fiabilité du service rendu par les SIC, et à mutualiser les SI. Elle est responsable de la rationalisation globale du parc applicatif et de la cohérence globale du POS du ministère.

La DGSIC s'assure en particulier de la qualité du dossier d'expression de besoin, de l'adéquation du plan de management (étatique) et du financement des coûts complets.

3.1.5. ***Direction interministérielle des systèmes d'information et de communication***

Le directeur interministériel des systèmes d'information et de communication oriente, anime et coordonne les actions des administrations de l'État visant à améliorer la qualité, l'efficacité, l'efficience et la fiabilité du service rendu par les SIC, et à mutualiser les projets.

Selon l'article 7. du décret n° 2006-497 du 2 mai 2006 de création du DISIC, tout projet de SI de fonctionnement supérieur à 9 M d'euros doit obtenir l'accord formel de la direction interministérielle des systèmes d'information et de communication (DISIC). Tout projet compris entre 5 et 9 M d'euros doit faire l'objet d'une information à la DISIC [arrêté du 1er juin 2011 (2)]. Ces montants sont évalués selon les règles précisées par le DISIC (T2, T3 et T5).

3.2. **En conduite de projet (jusqu'au stade d'utilisation).**

Une représentation schématique des articulations entre les acteurs de la conduite de projets fait l'objet de l'annexe II., figure 1. Les activités à réaliser sont détaillées en première partie de l'annexe III.

3.2.1. ***Responsable fonctionnel du projet.***

Le RF du projet porte le besoin fonctionnel pendant tout le cycle de vie du SI. Il coordonne l'ensemble des activités liées à l'expression de besoin fonctionnel, en s'appuyant sur les pilotes de processus métier, les groupes d'experts métier et les groupes d'utilisateurs. Il définit les cibles de déploiement et les performances attendues.

Le RF préside le comité des utilisateurs.

Il pilote et est responsable de la conduite du changement, de la formation, du déploiement (sous l'angle métier), des demandes d'évolution, de la stratégie de reprise des données et de l'assistance aux utilisateurs. Il doit garantir la qualité des données (reprises, gérées et produites par le SIC).

Sa responsabilité persiste pendant le stade d'utilisation.

3.2.2. ***Responsable de conduite de projet***

Le responsable de conduite de projet (RCP) est responsable de la conduite du projet. Il rend compte au CODIR (présidé par l'AC) de l'avancée du projet en termes de coûts, délais et performances. Il traduit ou fait traduire le besoin en spécifications fonctionnelles générales et détaillées, ainsi qu'en spécifications techniques.

Le RCP met en œuvre les décisions du CODIR projet. Il préside le comité de pilotage (COPIL) projet.

Il supervise et coordonne l'ensemble des activités du projet, notamment le suivi des prestations du réalisateur et de l'hébergeur. Il est responsable de l'emploi des compétences au sein de l'équipe de projet. Le RCP est un professionnel de la conduite de projet.

Il entretient l'historique des décisions concernant le projet et les justificatifs qui s'y rapportent. Il garantit la cohérence d'ensemble des documents produits et des actions réalisées.

Il s'appuie sur les compétences dont il a besoin dans l'ensemble du ministère ou à l'extérieur. Dans le cas de projet complexe il constitue une équipe de conduite de projet intégrée (ECPI) qu'il anime.

3.2.3. ***Responsable fonctionnel d'ensemble, responsable de conduite de projet d'ensemble.***

Lorsque plusieurs projets sont menés parallèlement pour instrumenter ou automatiser des processus liés :

- un responsable fonctionnel d'ensemble (RFE) est désigné pour assurer la cohérence fonctionnelle des différents projets ;

- un responsable de conduite de projet d'ensemble (RCPE) est désigné pour assurer la cohérence technique, calendaire et financière des différents projets.

RFE et RCPE ont autorité de coordination sur les RF et RCP correspondants. Ils rendent compte aux CODIR des différents projets de la coordination des projets.

3.2.4. ***Responsable de réalisation du projet.***

Le responsable de réalisation de projet (RRP) est responsable du développement, de l'intégration et du déploiement technique du SIC en projet.

Si le développement est externalisé, le RRP est le chef de projet chez l'industriel contractant. Si le développement est interne au ministère, le RRP appartient à l'entité responsable de la réalisation.

Il est responsable de la réalisation. La mise en place des moyens du déploiement peut également lui être confiée.

3.2.5. ***Conduite de projet intégrée - en réseau ou en équipe dédiée.***

Une conduite intégrée est assurée dès le lancement de la phase d'orientation du stade d'études. Elle perdure jusqu'à la fin du stade de développement (MSO).

L'ECPI rassemble les compétences permettant l'optimisation et la maîtrise du projet en termes de coûts, de délais et de performances. Elle est pilotée par le RCP, en liaison étroite avec le RF. Y sont nécessairement intégrés les rôles :

- d'architecte de système d'information (ASI) ;

- de responsable de sécurité des systèmes d'information projet (RSSI-P) : un RSSI-P est désigné pour piloter la démarche d'intégration de la sécurité des systèmes d'information (SSI) durant les deux premiers stades, jusqu'à l'homologation initiale incluse, qu'il est chargé d'instruire. Il assure également la phase de transfert de responsabilité vers le RSSI-Aval (RSSI-A) (3) lors des déploiements. Pour les cas où le volet SSI est important, il est appuyé par des experts SSI de métier au sein d'un groupe de travail de sécurité de système d'information (GTSSI) *ad hoc* instauré dès la phase d'orientation du stade d'études (décrit en annexe III. au point 1.3.) ;

- d'acheteur (représentant du pouvoir adjudicateur dans le cas de prestations externalisées) ;

- d'administrateur des données [administrateur des données système (ADD-SYS)] (cf. annexe V.) responsable notament de leur qualité ;

- de coordonnateur d'activités techniques (CAT), traitant des points relatifs à l'hébergement, à l'exploitation, aux réseaux, aux servitudes, etc. Les responsabilités du CAT sont détaillées dans le chapitre traitant de l'enrôlement (cf. annexe IV.).

Ces rôles peuvent être confiés à un ou plusieurs acteurs, nommément désignés, à temps partiel ou plein, selon la complexité et les spécificités du projet. La composition de l'ECPI peut évoluer dans le temps, en tant que de besoin, et sur proposition du RCP.

Les membres de l'ECPI partagent toutes les informations et proposent des décisions de façon conjointe.

Le RCP, en liaison avec le RF, assure la responsabilité d'organiser, planifier et mettre en œuvre toutes les activités nécessaires au déroulement du projet en appliquant notamment les règles et le cadencement décrits dans la présente instruction.

L'ensemble des acteurs de la conduite de projet doit impérativement respecter les directives ministérielles qui s'appliquent aux périmètres du projet et de leurs responsabilités (notamment celles référencées en annexe I.).

L'ECPI s'appuie sur des experts ou des groupes de travail (GT), permanents ou temporaires. Le rôle et le fonctionnement de ces GT sont décrits par le plan de management.

3.2.6. ***Comité des utilisateurs.***

En cas de besoin, certains projets complexes peuvent amener à la constitution d'un comité des utilisateurs. Dans le cas où ce comité n'est pas créé, l'AU principale en assume directement les responsabilités.

Le comité des utilisateurs, présidé par le RF, rassemble les représentants des AU ainsi que le RCP.

Les responsabilités du comité des utilisateurs sont :

- de vérifier que les exigences fonctionnelles sont bien prises en compte en participant aux travaux de spécifications générales et détaillées, en se prononçant sur l'ergonomie du système, en participant aux tests fonctionnels, et en validant l'aide en ligne, la documentation utilisateurs et la formation ;

- de préciser le besoin fonctionnel autant que de besoin ;

- de définir l'évolution des compétences métiers qui seront nécessaires au stade d'utilisation du système ;

- de faire remonter au COPIL et/ou au CODIR l'incidence sur les métiers des évolutions fonctionnelles et des arbitrages de la conduite du projet ;

- de proposer au COPIL les décisions ou arbitrages sur le plan fonctionnel ;

- de préparer et d'assister le déploiement sur le plan fonctionnel ;

- de traiter les observations de l'ensemble des utilisateurs ;

- de préparer et animer la « conduite du changement ».

3.2.7. ***Responsabilité de réalisation.***

Une maîtrise d'œuvre - interne ou externe - assure la réalisation du SI, suivant les règles en vigueur et les choix techniques définis par le RCP.

Elle prend à sa charge l'intégration technique et l'ensemble des interfaces du SI en intégrant les contraintes de la mise en œuvre du futur système dans son environnement.

3.2.8. ***Responsabilité de déploiement.***

En s'appuyant sur le CAT, le RCP s'assure la mise à disposition des moyens techniques nécessaires au déploiement du SI sur l'ensemble des sites concernés. Ces moyens peuvent être : l'énergie, la climatisation, l'emplacement des matériels, la sécurité physique, etc.

3.3. **Au stade d'utilisation.**

Une représentation schématique de l'articulation des acteurs de la conduite de SI au stade d'utilisation fait l'objet de l'annexe II., figure 2. Les activités à réaliser sont détaillées en deuxième partie de l'annexe III.

3.3.1. ***Responsable fonctionnel du système.***

Le RF est normalement le même qu'au stade de développement. Il est chargé de piloter les groupes d'utilisateurs. Le RF est le président du comité des utilisateurs. Il pilote la cohérence du système par rapport aux évolutions du besoin fonctionnel des utilisateurs. Le RF est responsable de l'évaluation de la satisfaction des utilisateurs.

Le RF est aussi président du comité de gestion de la configuration du système (cf. point 3.4.3.). À ce titre, il instruit les demandes d'évolution (y compris les évolutions majeures) et prépare les décisions du CODIR du système en exploitation, dont celles nécessitant un retour en mode projet.

3.3.2. ***Responsable technique de système.***

Le responsable technique de système (RTS) est responsable devant l'AC de la mise à disposition du système, de son maintien en condition opérationnelle (MCO), et de son maintien en condition de sécurité (MCS) en liaison avec le RSSI-A. Il s'assure du maintien de la qualité de service sur le plan technique. Il fait mettre en œuvre techniquement les évolutions décidées.

3.3.3. ***Responsable de sécurité des systèmes d'information aval.***

Le RSSI-A (3) est désigné par l'AC pour assurer le suivi SSI du système en service, jusqu'à son retrait. Le RSSI-A est notamment chargé d'instruire les renouvellements d'homologation [instruction n° 900/DEF/CAB du 18 juin 2007 modifiée [IM 900] (4)].

Pour le système dont il a la charge et dans le domaine de la SSI, il conseille, recommande et propose au RF et au RTS des règles spécifiques ; il est le garant de la cohérence des mécanismes et procédures de sécurité.

3.3.4. ***Maintien en condition opérationnelle.***

La fonction de MCO réalise les modifications applicatives du système en exploitation et de ses interfaces, qui relèvent du stade d'utilisation. Elle a en charge :

- la conservation des performances du système en exploitation, par des actions de maintenance sur instruction conjointe du RF et du RTS ;

- le traitement des incidents, pour le domaine applicatif ;

- la gestion et la réalisation des demandes de changement, pour la partie applicative liée au système en exploitation.

Les évolutions majeures (évolution lourde du périmètre fonctionnel, refonte technique etc.) sont traitées comme de nouveaux projets.

3.3.5. ***Fonction d'exploitation.***

Cette fonction assure l'exploitation et la supervision quotidiennes du système, ainsi que la gestion des incidents et des changements, matériels ou logiciels, relatifs au fonctionnement du SI.

3.3.6. ***Fonction de soutien aux utilisateurs.***

La fonction de soutien aux utilisateurs assure l'ensemble des relations avec les utilisateurs finaux des systèmes en exploitation. Elle comprend également l'assistance, le conseil, le recueil, et la résolution des incidents de son niveau, la prise en compte et la pré-qualification des autres incidents et/ou demandes d'évolutions.

3.4. **Instances de décision et d'examen.**

3.4.1. ***Comité de direction du projet puis du système en exploitation.***

La mise en place d'un CODIR est systématique à partir de la phase d'orientation du stade d'études.

Le CODIR est chargé de superviser la conduite du projet, puis du système, et la réalisation de ses objectifs. Il permet également d'assurer le partage et la transparence des informations au sein du ministère de la défense et des anciens combattants.

Le CODIR se réunit au moins semestriellement en mode projet, puis annuellement en stade d'utilisation. Il peut se réunir également sur demande de ses membres pour un besoin d'arbitrage urgent ou l'étude de choix majeurs. Il est l'instance de décision associée au passage d'étapes obligatoires, notamment la décision de déploiement et celle de MSO.

Sur proposition du comité de gestion de configuration (cf. point 3.4.3.), il qualifie les évolutions nécessitant la création d'un nouveau projet pour la prise en compte d'évolutions majeures.

Le CODIR est composé, au minimum, des membres suivants :

- l'AC, qui en assure la présidence ;

- les AU ;

- le RF du projet et le RCP (jusqu'au stade de développement inclus), puis le RTS et le RF du système (à partir du stade d'utilisation) qui en assurent l'animation ;

- les représentants des structures de soutien concernées ;

- le représentant du pouvoir adjudicateur, le cas échéant ;

- le (ou les) RZF concerné(s) si nécessaire ;

- et si le projet fait partie d'un projet d'ensemble, le RCPE et le RFE.

La DGSIC et le responsable de budget opérationnel de programme (RBOP) concerné sont tenus informés de ces réunions, et destinataires de leurs relevés de conclusions. Ils peuvent s'y faire représenter.

3.4.2. ***Comité de pilotage du projet.***

Le COPIL du projet, présidé par le RCP, rassemble le RF du projet et l'ensemble de l'ECPI, ainsi que les compétences ou experts nécessaires en tant que de besoin. Il convoque le RRP et les experts techniques et fonctionnels nécessaires au projet en tant que de besoin.

Le COPIL, subordonné au CODIR :

- valide les décisions technico-fonctionnelles « courantes » proposées par l'ECPI ;

- prépare et de propose les décisions au CODIR ;

- assure la cohérence d'ensemble du projet ;

- s'assure du partage des informations ;

- s'assure de l'application du plan de management ;

- s'assure et rend compte de la tenue des objectifs en termes de fonctionnalités - performances - coûts - délais - sécurité.

3.4.3. ***Comité de gestion de la configuration du système.***

Le comité de gestion de la configuration du système en utilisation, présidé par le RF, rassemble le RF, le RTS, et dans le cas de SI complexe l'ensemble des membres de la direction du système (RSSI-A, représentants des formateurs et groupes utilisateurs, cf. figure 2 annexe II.), et les représentants des équipes d'exploitation, de MCO et de soutien aux utilisateurs. Il convoque les experts techniques et fonctionnels selon l'ordre du jour.

Le comité de gestion de la configuration du système :

- valide les décisions fonctionnelles et techniques du système en utilisation de son niveau (qui n'interfèrent pas avec celles du CODIR) ;

- s'assure du respect des objectifs de qualité et de disponibilité de service du système ;

- s'assure l'application du plan de management ;

- instruit les demandes d'évolution (y compris les évolutions majeures, nécessitant un retour en mode projet) ;

- prépare les décisions du CODIR.

3.4.4. ***Commission d'homologation du projet puis du système en exploitation.***

Tout SI doit être homologué par l'autorité « qualifiée » (AQ) désignée. Cette homologation est instruite par le RSSI-P ou le RSSI-A.

La commission d'homologation (CH) (conformément aux textes SSI en vigueur) émet un avis motivé sur la capacité du SI livré et déployé à traiter les informations protégées au niveau de sécurité requis. Mise en place à partir de la phase d'orientation, elle prépare et conduit le processus d'homologation du projet.

3.4.5. ***Groupe de travail d'examen de projet - groupe d'instruction des systèmes.***

Les modalités d'examen des systèmes d'information et de communication sont définies par l'instruction n° 2005/DEF/DGSIC du 22 juillet 2010 [IM 2005].

3.5. **Opérateur.**

L'opérateur assure l'ensemble des responsabilités d'hébergement, d'infogérance et d'une partie du soutien aux utilisateurs pour les SIC au cours du stade d'utilisation.

L'opérateur doit être sollicité dès les premiers stades, comme expert de l'exploitation et du soutien SIC de manière générale, au profit du projet, pour en préparer le stade d'utilisation, lors de l'enrôlement du SI.

Il doit être également sollicité en tant que fournisseur de services SIC (cf. catalogue ministériel des services), tels que la mise à disposition d'un environnement de pré-production et/ou de production.

L'opérateur est représenté au sein de l'ECPI, par le CAT désigné.

À partir du stade d'utilisation, après la MSO, lorsqu'elles en ont la charge, les structures de soutien réalisent ou font réaliser les activités de MCO et/ou de MCS applicatif et matériel.

3.6. **Sécurité des systèmes d'information.**

La SSI doit être prise en compte dès le démarrage du projet SIC et jusqu'à son retrait conformément aux objectifs de sécurité et aux textes SSI en vigueur. Les actions liées à la SSI sont synthétisées dans cette instruction. Une description plus précise de ces actions est fournie dans le guide SSI [Guide SSI].

Les principaux acteurs sont l'AQ, l'autorité d'homologation (AH), et les RSSI-P et RSSI-A.

Tout système doit être homologué ou obtenir une homologation provisoire d'exploitation avant utilisation.

3.6.1. ***Autorité qualifiée.***

L'AQ de sécurité des SI (SSI) est responsable de la SSI pour les organismes relevant de son autorité, ainsi que pour les systèmes dont elle a directement la charge.

L'AQ SSI assume les responsabilités énoncées à l'article 88 de l'instruction générale interministérielle n° 1300/SGDN/PSE/SSD du 23 juillet 2010 (IGI 1300 [ARR03]) (4). Elle est notamment chargée :

- d'assurer ou de faire assurer le MCS des systèmes dont elle a la charge ;

- d'organiser le processus d'homologation et de désigner les autorités d'homologation de ses systèmes ;

- d'évaluer, au regard des objectifs de sécurité, le niveau général de sécurité de ses systèmes.

3.6.2. ***Autorité d'homologation.***

L'AQ SSI peut déléguer l'homologation à une AH. La délégation fixe les limites des attributions correspondantes et précise le niveau de confidentialité maximal ainsi que le périmètre d'application pour lequel chaque AH est compétente.

3.7. **Contrôle financier.**

3.7.1. ***Responsable de budget opérationnel de programme.***

Les RBOP vérifient la provision des ressources financières nécessaires aux projets puis aux systèmes en exploitation.

3.7.2. ***Comité ministériel d'investissement.***

Suivant des seuils déterminés (50 M d'euros pour les SI hors opération d'armement), les dossiers de franchissement de stade de certains projets et les grandes décisions structurantes sont éventuellement proposés à l'ordre du jour du comité ministériel d'investissement (CMI).

3.7.3. ***Commission exécutive permanente.***

Pour ce qui concerne les projets régis par la présente instruction, la commission exécutive permanente (CEP) n'intervient que sur les activités budgétaires réservées, et formule un avis sur la libération des autorisations d'engagement (AE).

Les projets ou systèmes relevant d'une activité budgétaire réservée doivent faire l'objet d'un examen en groupement de travail d'examen de projet (GTEP) ou en groupe d'instruction des systèmes (GIS) et obtenir un avis favorable préalablement à la présentation de l'activité en CEP.

La liste des activités réservées est entretenue par la CEP et publiée en fin d'année pour l'année suivante. La date de présentation en CEP est fixée par le RBOP.

4. CONDUITE DES PROJETS.

4.1. **Démarche détaillée.**

L'annexe III. détaille les activités à mener dans le cadre du cycle de vie des systèmes d'information de fonctionnement (SIF).

Les RCP doivent s'y appuyer pour architecturer le déroulé de la conduite de leurs projets, en fonction des enjeux et des risques de ceux-ci. Les plans de management décrivent, entre autres, ce qui doit être formalisé.

4.2. **Exigences réglementaires.**

Certains points méritent un traitement et une formalisation systématiques.

Tel est le cas des livrables et des jalons imposés dans le cadre du contrôle exercé par les instances spécialisées (GTEP/GIS). L'instruction n° 2005/DEF/DGSIC du 22 juillet 2010 [IM 2005] en liste les exigences.

Dans certains domaines les projets sont en outre soumis à une réglementation particulière. C'est par exemple le cas de la SSI [cf. instruction ministérielle 900 (4)], mais aussi de l'opérateur (cf. annexe IV. sur l'enrôlement des SI), de l'administration des données (cf. annexe V.), ou encore de la protection de la vie privée [cf. annexe VI. sur la commission nationale de l'informatique et des libertés (CNIL)].

4.3. **Livrables obligatoires.**

Outre les livrables imposés réglementairement, dans le cadre strict de l'activité de conduite de projet de SIF, les éléments suivants doivent être produits :

- expression de besoin structuré selon le modèle « Expression de besoin SIC » [TYP 001] ;

- plan de management (PM), qui devra être validé par l'AC afin de vérifier l'adéquation de celui-ci à la complexité du projet, à ses enjeux et à ses risques ;

- cahier de charge fonctionnel (CdCF), qui peut être dans les cas très simples une reprise de l'expression de besoin ;

- évaluation de la charge des ressources humaines (RH) et financière ainsi que le calendrier de mise en œuvre ;

- dossier d'exigences couvertes et validées par la maîtrise d'œuvre (MOE) ;

- besoins d'hébergement (cf. annexe IV.) ;

- procès verbaux des recettes ;

- documentation prévue dans le PM, dont les documents techniques et utilisateurs ;

- plan de déploiement ;

- plan de formation ;

- le SIC opérationnel ;

- contrat de service avec l'hébergeur (cf. annexe IV.) ;

- procès-verbal (PV) de retrait de service.

5. DISPOSITIONS PARTICULIÈRES.

5.1. **Projet d'ensemble.**

Un projet d'ensemble rassemble, sous l'autorité d'un RCPE et d'un RFE, plusieurs projets concomitants ou successifs concourant à la satisfaction d'un besoin complexe.

La création d'un projet d'ensemble fait l'objet d'une décision prise en comité exécutif du conseil des SIC (CECSIC) qui en fixe le périmètre.

L'organisation et le financement mis en place pour chaque projet d'ensemble font l'objet d'une décision particulière du DGSIC.

5.2. **Urgence opérationnelle.**

L'acquisition d'un SI en procédure d'urgence opérationnelle doit demeurer exceptionnelle. La décision du recours à la procédure « d'urgence opérationnelle » est prise par le chef d'état-major des armées (CEMA) en liaison avec l'opérateur qui tient informés la DGSIC et le GTEP/GIS.

Dès que les conditions le permettent, le projet reprend les modalités de la présente instruction et un bilan de l'impact des dérogations adoptées est établi. L'impact financier, technique et capacitaire est établi par ailleurs.

Pour le ministre de la défense et des anciens combattants et par délégation :

Le directeur général des systèmes d'information et de communication,

Christian PÉNILLARD.

Le général de brigade,
directeur adjoint de la direction générale des systèmes d'information et de communication,

Bertrand LAHOGUE.

---

(1) Les programmes et opérations d'armement sont régis par l'instruction 1516 (INS08).

(2) n.i. BO.

(3) Les rôles des RSSI-P et RSSI-A sont définis par l'instruction ministérielle 900 [IM 900]

(4) n.i. BO.

ANNEXE I.

TEXTES DE RÉFÉRENCE ET GLOSSAIRES.

1. DOCUMENTS APPLICABLES.

[CP] : code pénal (1).

[CNIL] : loi n° 78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés.

[DEC DGSIC] : décret n° 2006-497 du 2 mai 2006 portant création de la direction générale des systèmes d'information et de communication et fixant l'organisation des systèmes d'information et de communication du ministère de la défense.

[ARR 2006] : arrêté du 6 juin 2006 portant création et organisation d'instances relatives aux systèmes d'information et de communication du ministère de la défense.

[ARR DGSIC] : arrêté du 15 février 2011 portant organisation de la direction générale des systèmes d'information et de communication.

[ARR DISIC] : arrêté du 1er juin 2011 (1) pris pour application de l'article 7. du décret n° 2011-193 du 21 février 2011 (1) portant création d'une direction interministérielle des systèmes d'information et de communication de l'État.

[CIRC] : circulaire du 16 septembre 1996 du Premier ministre relative aux schémas directeurs des systèmes d'information et de télécommunication.

[IGI 1300] : instruction générale interministérielle n° 1300/SGDN/PSE/SSD du 23 juillet 2010 (1) portant approbation sur la protection du secret de la défense nationale.

[IM 954] : instruction n° 954/DEF/SGA du 13 septembre 1994 concernant l'application au ministère de la défense des dispositions de la 1oi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[IM 2005] : instruction n° 2005/DEF/DGSIC du 22 juillet 2010 relative aux modalités d'examen des systèmes d'information et de communication.

[IM 1516] : instruction n° 1516/DEF/DGA/DP/SDM du 26 mars 2010 relative au déroulement et la conduite des opérations d'armement.

[IM 22912] : instruction n° 22912/DEF/SGA/DAJ/D2P du 26 mars 2010 relative à la gouvernance des investissements du ministère de la défense.

[IM 900] : instruction n° 900/DEF/CAB/DR du 18 juin 2007 (1) modifiée, relative à la protection du secret de la défense nationale au sein du ministère de la défense.

[NOTE 239] : note n° 239/DEF/EMA/EPI/PSIOC/NP du 18 mars 2010 (1) relative à l'urbanisation des systèmes d'information et de communication opérationnels et à la place et rôle des responsables de zone fonctionnelle.

[NOTE 582] : note n° 582/DEF/DGSIC/BAG du 20 mai 2011 (1) relative à l'organisation de la DGSIC.

[Guide SSI] : « GUIDE SSI » - en cours de validation.

[TYP 001] : « Expression de besoin SIC » (EBSIC), document type - en cours de validation.

[PHARE] : méthode PHARE.

2. DIRECTIVES MINISTÉRIELLES.

[DGSIC 001] : directive n° 1/DEF/DGSIC du 8 novembre 2006 (1) portant sur les logiciels du ministère de la défense.

[DGSIC 002] : directive n° 2/DEF/DGSIC du 9 mars 2007 modifiée, portant sur le système d'annuaires (SA) du ministère de la défense.

[DGSIC 003] : directive n° 3/DEF/DGSIC du 8 janvier 2008 définissant les règles de la messagerie électronique.

[DGSIC 004] : directive n° 4/DEF/DGSIC du 27 septembre 2007 portant les règles d'emploi du plan d'occupation des sols de la démarche d'urbanisation des systèmes d'information et de communication du ministère de la défense.

[DGSIC 005] : directive n° 5/DEF/DGSIC du 7 avril 2008 portant sur les système de gestion de base de données relationnelle (SGBDR).

[DGSIC 006] : directive n° 6/DEF/DGSIC du 5 décembre 2008 relative aux composants de logiciels décisionnels.

[DGSIC 007] : directive n° 7/DEF/DGSIC du 13 janvier 2009 portant sur la téléphonie sur le protocole IP.

[DGSIC 008] : directive n° 8/DEF/DGSIC du 29 juin 2009 modifiée, définissant les règles à appliquer au système de postes terminaux.

[DGSIC 009] : directive n° 9/DEF/DGSIC du 2 juillet 2009 portant sur les données géographiques et hydrographiques sous formes numériques.

[DGSIC 010] : directive n° 10/DEF/DGSIC du 5 novembre 2009 sur la prévention contre les codes malveillants.

[DGSIC 011] : directive n° 11/DEF/DGSIC du 8 janvier 2010 portant sur la sécurisation des autocommutateurs.

[DGSIC 012] : directive n° 12/DEF/DGSIC du 1er juin 2010 portant sur la mobilité.

[DGSIC 013] : directive n° 13/DEF/DGSIC du 30 juin 2010 portant sur la sécurité des accès aux services de l'internet et la sécurité de l'hébergement des services internet du ministère.

[DGSIC 014] : directive n° 14/DEF/DGSIC du 19 juillet 2010 portant sur l'administration des données du ministère de la défense.

[DGSIC 015] : directive n° 15/DEF/DGSIC du 10 novembre 2010 portant sur la réalisation des audits de sécurité des systèmes d'information au sein du ministère de la défense (DIR-AUDITS).

3. SITES DE RÉFÉRENCE.

[Site DGSIC] : site DGSIC à l'adresse intradef ; www.dgsic.defense.gouv.fr.

[Site SSI] : site SSI à l'adresse intradef ; www.ssi.defense.gouv.fr.

A1.

Méthode PHARE.

4. TABLE DES ACRONYMES.

SIGLE.	DÉFINITION.
AC	Autorité cliente.
ADD	Administration des données.
ADD-DEF	Administration des données de défense.
ADD-SYS	Administrateur de données du système.
ADD-ZF	Administration des données de zone fonctionnelle.
ADD-SYD	administrateur des données système.
AH/AHP	Autorité d'homologation/autorité d'homologation principale.
AQ	Autorité qualifiée (SSI).
ASI	Architecte de système d'information.
AU	Autorité utilisatrice.
BOP	Budget opérationnel de programme.
CAT	Coordonateur d'activités techniques.
CCTP	Cahier des clauses techniques particulières.
CdCF	Cahier des charges fonctionnel.
CECSIC	Comité exécutif du conseil des SIC.
CEMA	Chef d'état-major des armées.
CEP	Commission exécutive permanente.
CGA	Contrôle général des armées.
CH	Commission d'homologation (SSI).
CMI	Comité ministériel d'investissement.
CNIL	Commission nationale informatique et libertés.
CODIR	Comité directeur.
COPIL	Comité de pilotage.
COVESIOC	Comité de convergence des systèmes d'information opérationnels et de communication.
CSIC	Conseil des SIC.
CTSIC	Commission technique des SIC.
DAF	Direction des affaires financières.
DGA	Direction générale de l'armement.
DGSIC	Direction générale des systèmes d'information et de communication.
DIRISI	Direction interarmées des réseaux d'infrastructure et des systèmes d'information.
DISIC	Direction interministérielle des SIC.
DRS	Dossier de retrait de service.
ECPI	Équipe de conduite de projet intégrée.
EMA	État-major des armées.
EO	Étude d'opportunité.
FEB	Fiche d'expression de besoin.
FEROS	Fiche d'expression rationnelle des objectifs de sécurité.
GT	Groupe de travail.
GTEP	Groupe de travail d'examen de projets.
GTEP-GIS	Groupe de travail d'examen de projets - groupe d'instruction des systèmes.
IGC	Infrastructure de gestion de clés.
LID	Lutte informatique défensive.
MCO	Maintien en condition opérationnelle.
MCS	Maintien en condition de sécurité.

MDD-SYS	Modèle de données système.
MDT-ZF	Modèle de données transverses de zone fonctionnelle.
MOE	Maîtrise d'œuvre.
MSO	Mise en service opérationnel.
OME	Outre-mer et à l'étranger.
PCI	Plan de continuité informatique.
PES	Procédures d'exploitation de la sécurité.
PM	Plan de management.
POS	Plan d'occupation des sols.
PSS	Politique de sécurité du système.
PV	Procès-verbal.
RBOP	Responsable de BOP.
RCP	Responsable de conduite de projet.
RCPE	Responsable de conduite de projet d'ensemble.
RETEX	Retour d'expérience.
RF	Responsable fonctionnel.
RFE	Responsable fonctionnel d'ensemble.
RH	Ressources humaines.
RQF	Responsable de quartier fonctionnel.
RRP	Responsable de réalisation du projet.
RSSI - OSSI	Responsable de la sécurité des SI - officier de sécurité des SI.
RTS	Responsable technique de système.
RZF	Responsable de zone fonctionnelle.
SDISI	Sous-direction de l'ingénierie des systèmes d'information (de la DGSIC).
SGA	Secrétariat général pour l'administration.
SI	Système d'information.
SIAG	Systèmes d'information d'administration et de gestion.
SIC	Systèmes d'information et de communication.
SIOC	Systèmes d'information opérationnels et de communication.
SSI	Sécurité des systèmes d'information.
STB	Spécification technique de besoin.
STC-IA	Socle technique commun interarmées.
TME	Tierce maintenance d'exploitation.
VABF	Vérification d'aptitude au bon fonctionnement.
VAR	Variation annuelle du référentiel.
VSR	Vérification de service régulier.
ZF	Zone fonctionnelle.

5. DÉFINITIONS.

Plan de management.

Le plan de management est un document évolutif. Il est créé dès la phase d'initialisation du stade d'études et suit tous les stades du projet. Il reste actif lors du stade d'utilisation du système. Son rôle est d'être le document de référence sur l'ensemble du cycle de vie du système.

Le plan de management comporte, *a minima*, les éléments suivants :

- présentation du projet (enjeux, objectifs, limites et contraintes) ;

- organisation et fonctionnement des acteurs en charge de la réalisation des travaux ;

- démarche de conduite ;

- modalité de suivi des travaux ;

- analyse et gestion des risques ;

- maîtrise de la qualité, des coûts et des délais ;

- gestion de la SSI ;

- gestion de la configuration ;

- liste des documents devant être formalisés.

Suivant la complexité du projet/système, le plan de management est complété en tant que de besoin de manière à ce que celui-ci soit un fil conducteur fiable.

L'établissement et la tenue à jour du plan de management relèvent de la responsabilité du RCP, puis du RF du système.

Schéma directeur de secteur fonctionnel.

Selon l'annexe de la note n° 275/DEF/DGSIC/SDMA/BGAI du 14 mars 2011 (1), tout « responsable de secteur fonctionnel (RZF ou RQF) doit piloter la cohérence des SIC de son secteur, qui s'adosse naturellement sur une vision métier ministérielle. ».

En particulier, « il est chargé de rédiger le schéma directeur opérationnel métier (ou encore schéma directeur de secteur fonctionnel) propre à son secteur, qui décrit en particulier le programme d'actions (fonctionnelles, organisationnelles, techniques, financières, etc.) à entreprendre pour atteindre la cible, de le mettre en œuvre et de le suivre en procédant annuellement à sa mise à jour. ».

Pour fiabiliser la cohérence et atteindre les résultats attendus des actions planifiées par les RZF/RQF, toute expression de besoin devra faire référence à un schéma directeur de secteur fonctionnel.

Infogérance.

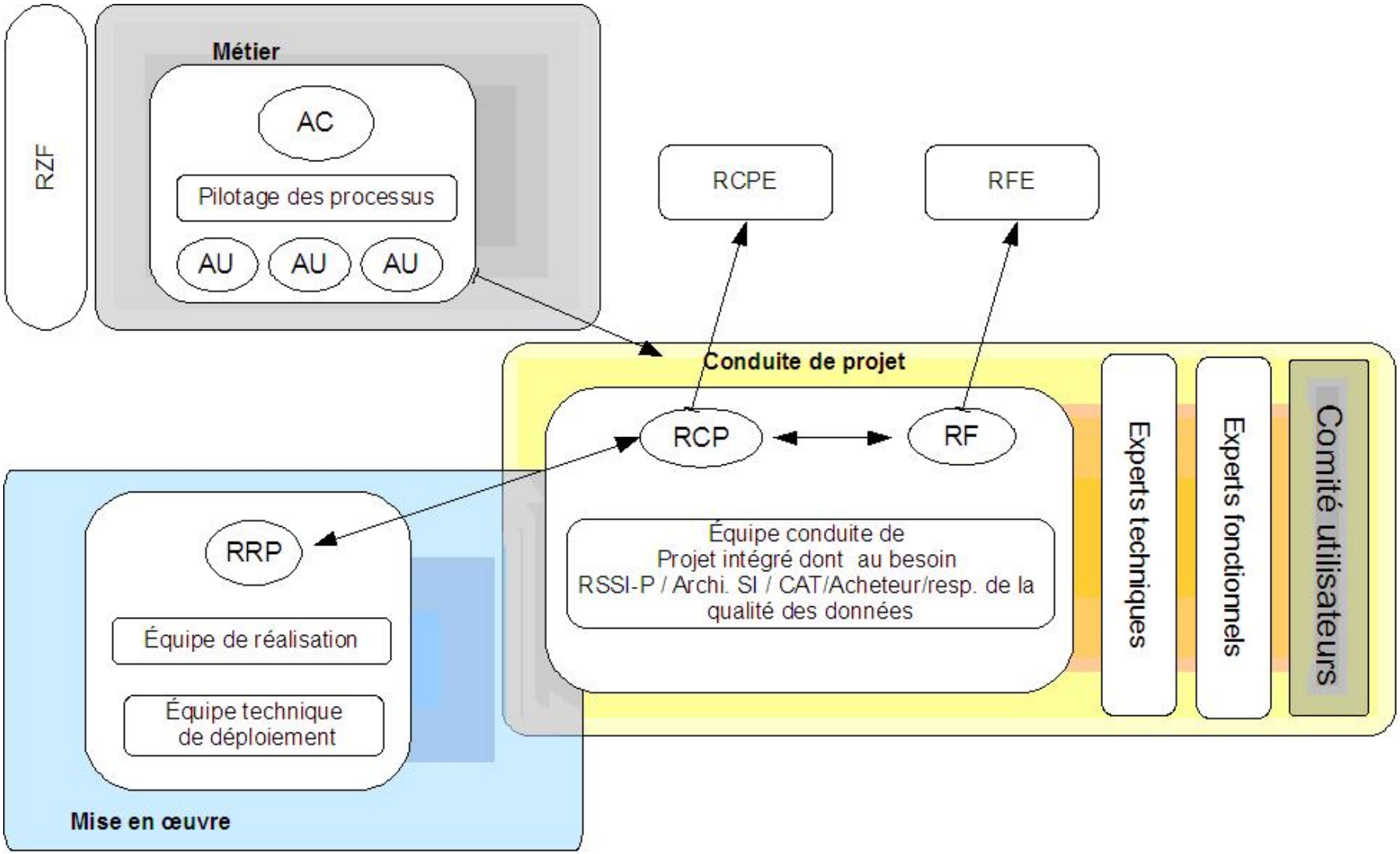
On appelle infogérance l'ensemble des opérations qui consistent à déléguer tout ou partie de la fonction informatique de l'opérateur à des prestataires externes spécialisés. Ces prestataires assurent alors la pérennité de l'activité informatique, la maintenance du parc ainsi que la mise à niveau des programmes durant une période définie par contrat.

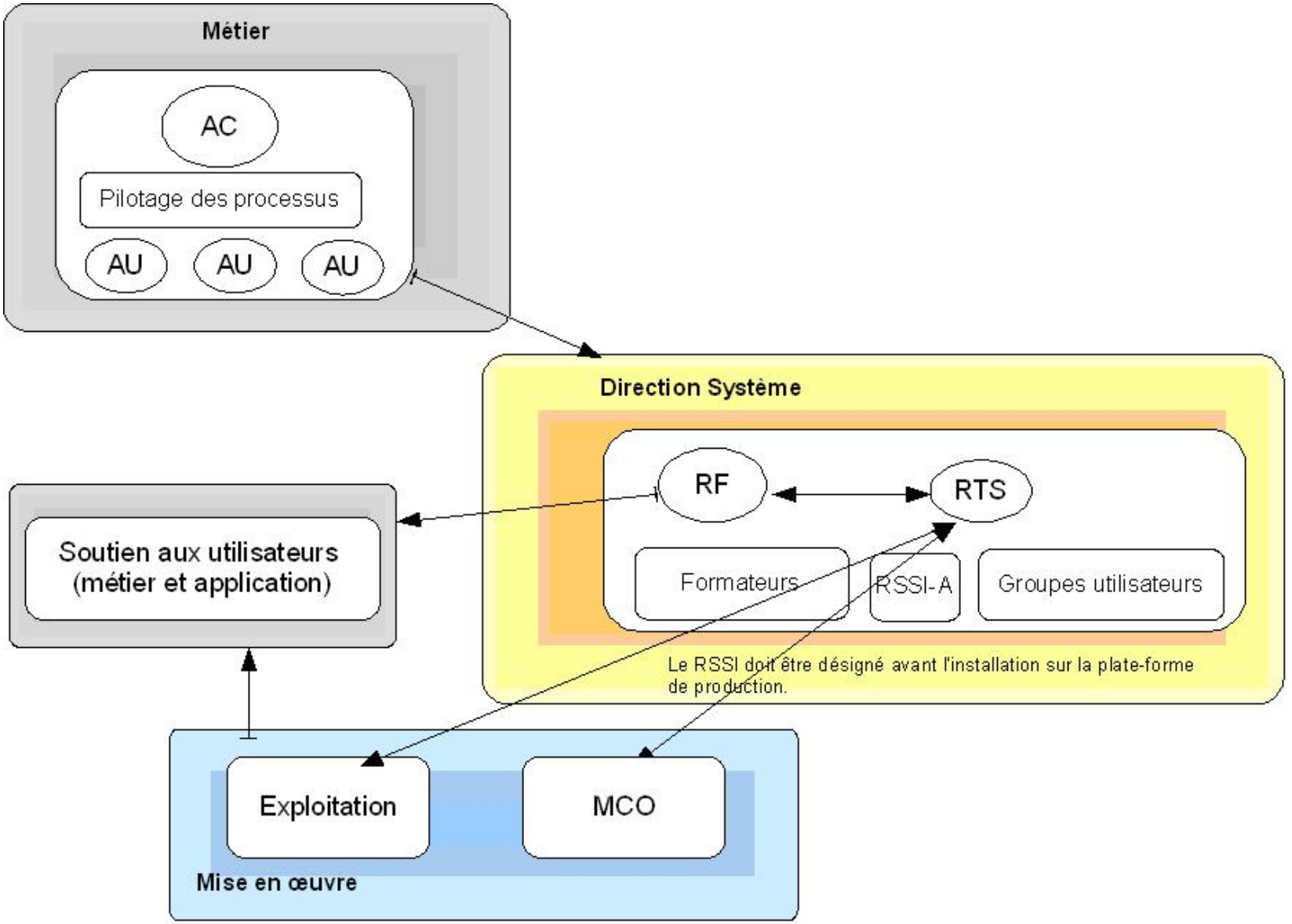
---

(1) n.i. BO.

ANNEXE II.

SYNOPSIS DES RÔLES.


RZF
Métier
AC
Pilotage des processus
AU
AU
AU
RCPE
RFE
Conduite de projet
RCP
RF
Équipe conduite de
Projet intégré dont au besoin
RSSI-P / Archi. SI / CAT/Acheteur/resp. de la
qualité des données
Experts techniques
Experts fonctionnels
Comité utilisateurs
RRP
Équipe de réalisation
Équipe technique
de déploiement
Mise en œuvre


Métier
AC
Pilotage des processus
AU
AU
AU
Direction Système
RF
RTS
Formateurs
RSSI-A
Groupes utilisateurs
Le RSSI doit être désigné avant l'installation sur la plate-forme de production.
Soutien aux utilisateurs (métier et application)
Exploitation
MCO
Mise en œuvre

ANNEXE III.

CYCLE DE VIE.

L'ensemble des activités détaillées constituant les stades suivants (des études au retrait de service) doivent être réalisées en fonction du plan de management validé par l'AC, des directives générales et particulières spécifiques aux différents segments SIC, et notamment celles concernant la sécurité, l'architecture technique et l'administration des données.

Ces « activités projet » sont précédées de travaux préparatoires, internes aux organismes métier, et dont le résultat sera le point d'entrée du stade d'études.

Les activités ci-dessous doivent être menées à leur juste besoin en fonction de la complexité du projet, et conformément au plan de management.

1. STADE D'ÉTUDES.

La responsabilité de ce stade incombe à l'AC.

1.1. **Objectifs.**

Réunir les éléments nécessaires à une prise de décision sur l'intérêt de lancer un projet dans le contexte du (ou des) secteur(s) fonctionnel(s) sur lequel (lesquels) il se positionne.

Exprimer clairement le besoin métier.

Organiser les ressources nécessaires au déroulement du projet.

Spécifier les caractéristiques techniques générales du SIC réalisable et satisfaisant les besoins métier.

Aboutir à un choix de solution technique documenté, répondant à tout ou partie des exigences spécifiées, dans un périmètre déclaré « fonctionnel ».

Amener tous les risques en-deçà d'un seuil acceptable pour passer au stade de développement.

1.2. **Déclenchement de l'entrée dans le stade.**

Demandes émises par les autorités utilisatrices selon des modalités spécifiques à chacune.

Disponibilité d'une description de l'organisation et des processus métier à outiller.

1.3. **Activités.**

Phase de préparation :

- déterminer les objectifs du projet (vis-à-vis des opportunités stratégiques), son périmètre et sa faisabilité ;

- vérifier l'opportunité de lancement du projet dans le cadre de l'exécution du (ou des) schéma(s) directeur(s) du (ou des) secteur(s) fonctionnel(s) concerné(s).

Conditions obligatoires pour passer aux activités suivantes :

- accord obligatoire du RZF sur l'opportunité du projet et sur son positionnement ;

- nomination d'un RCP et d'un RF pour le projet par les instances définies au point 3.

Phase d'initialisation :

- domaine de l'expression de besoin métier (RF) du projet :

  - déterminer les objectifs du projet, analyser et formaliser les exigences et attentes du client [besoins explicites et implicites (1)] ;

  - décliner les exigences en objectifs quantifiés (sécurité, performance, fiabilité, exploitabilité, maintenabilité, portabilité, robustesse, ergonomie, etc.) ;

  - identifier, catégoriser et classer les informations manipulées par le futur SIC ;

- domaine de l'identification et de l'organisation des ressources selon la complexité du projet (RCP) :

  - déterminer l'organisation du projet (humaine et matérielle) ;

  - établir un plan de management (PM) préliminaire (obligatoire) ;

  - réaliser un planning macroscopique des tâches du projet (calendrier des rendez-vous majeurs) ;

  - définir le budget prévisionnel du projet ou une estimation de la charge en cas de développement interne ;

  - déterminer les moyens de contrôle (sur la gestion du projet) ;

  - analyser les menaces et dispositions envisagées pour les contrer ;

  - exprimer les premiers besoins d'hébergement (cf. annexe IV.) ;

- domaine SSI (cf. Guide SSI) :

  - informer l'autorité qualifiée et l'instance *ad hoc* de l'existence du projet ;

  - faire procéder à la désignation de l'autorité d'homologation si les textes réglementaires ne l'ont pas prévu ;

  - déterminer le niveau d'objectifs SSI du système d'information en projet ;

  - décider du type de démarche de sécurisation à mener (simplifiée ou non) ;

  - élaborer la stratégie d'homologation dans le cas d'une démarche simplifiée ;

  - vérifier l'opportunité d'une déclaration à la CNIL (cf. annexe VI.).

Validation obligatoire par le GTEP/GIS-J1 de l'exploitabilité de l'expression du besoin métier et de la pertinence de l'organisation du projet avant de passer aux activités suivantes.

Phase d'orientation :

- définir les architectures fonctionnelle et technique (en cohérence avec la cartographie des processus et les POS fonctionnels et applicatifs) ;

- procéder aux désignations/nominations des acteurs du projet ;

- élaborer une doctrine d'emploi ;

- domaine SSI (démarche non simplifiée) :

  - créer une fiche dans l'outil métier de la SSI ;

  - réaliser une première analyse de risques pour déterminer les objectifs de sécurité et formaliser les conclusions dans une fiche d'expression rationnelle des objectifs de sécurité (FEROS) exploratoire ;

  - saisir la DGSIC en cas d'interconnexion du SI avec un autre extérieur au ministère ;

- domaine SSI (démarche simplifiée) :

  - créer une fiche dans l'outil métier de la SSI ;

- évaluer l'impact sur l'organisation et le POS ;

- établir une analyse des risques internes et externes au projet ;

- estimer le coût du projet (en calculant le coût global de possession et en incluant une valorisation de l'impact sur l'organisation) ;

- identifier les modalités de reprise des données ;

- identifier les modalités de conduite de déploiement et du changement ;

- élaborer une stratégie d'acquisition ;

- consolider les demandes d'hébergement (cf. annexe IV.) ;

- préparer le contrat d'opération (cf. annexe IV.).

Conditions obligatoires pour passer aux activités suivantes :

- apprécier l'analyse des risques effectuée (notamment la stabilisation des exigences technico-fonctionnelles issues du besoin métier en GTEP/GIS-J2, ou GTEP/GIS-J5 s'il s'agit d'une évolution majeure) ;

- atteindre un accord sur la démarche contractuelle ;

- initialiser la dite démarche ;

- valider les ressources financières ou de développement interne allouées ;

- publication d'un appel d'offre dans le cas d'une externalisation.

Phase d'élaboration :

- finaliser les architectures fonctionnelle et technique (en cohérence avec la cartographie des processus, les POS fonctionnels et applicatifs, et les conditions de prise en charge du futur hébergeur) ;

- domaine SSI (démarche non simplifiée) :

  - rédiger la stratégie d'homologation ;

- réaliser une analyse de risques complète prenant en compte les conclusions de la phase précédente et formaliser ses conclusions dans une FEROS de référence ;

- définir la politique de sécurité du système (PSS) ;

- définir les éléments du MCS ;

- valider le plan de sécurité préliminaire élaboré par la MOE ;

- demander une prestation d'audit de sécurité ;

- demander une prestation d'évaluation des produits de sécurité si nécessaire ;

- demander une prestation d'analyse de sécurité de produits civils (ASPC) si nécessaire ;

- domaine SSI (démarche simplifiée) :

- rédiger les exigences de sécurité ;

- demander une prestation d'audit de sécurité ;

- initier la spécification des tests de réception [vérification d'aptitude au bon fonctionnement (VABF), vérification de service régulier (VSR)] ;

- mettre à jour les prévisions de consommation de ressources humaines et financières ;

- élaborer la stratégie de reprise de données (reprise, archivage et destruction) ;

- valider le plan d'organisation de développement (POD) ;

- réaliser une ou plusieurs maquettes (si besoin) ;

- finaliser les besoins d'hébergement (cf. annexe IV.) ;

- affiner le contrat d'opération (cf. annexe IV.) ;

- préparer l'intégration du SI avec l'opérateur (cf. annexe IV.).

1.4. **Éléments produits intermédiaires et/ou de sortie (suivant le plan de management).**

Expression de besoin structuré (évaluation de la valeur ajoutée, analyse des risques inhérents au lancement du projet ou à sa non-réalisation, etc.), selon le modèle « Expression de besoin SIC » en référence [TYP001].

PM.

Fiche d'expression de besoin (FEB) (si besoin).

Dossier de consultation aux entreprises (DCE) ou CdCF/STB.

Stratégie d'acquisition (si besoin) précisant notamment le calendrier de la consultation.

Doctrine d'emploi.

Charge de développement interne évaluée et calendrier de mise en œuvre.

FEROS exploratoire et de référence.

Acte d'engagement.

Dossier d'exigences couvertes et validées.

Stratégie d'homologation.

Exigences de sécurité.

PSS.

Politique de sécurité (PDS) et POD préliminaires (de responsabilité MOE).

Besoins d'hébergement (cf. point 3.3.).

1.5. **Déclenchement de sortie du stade.**

Choix d'une solution technique du CODIR.

2. STADE DE DÉVELOPPEMENT.

La responsabilité de ce stade incombe au RCP. Les travaux peuvent être réalisés par itérations successives des phases de ce stade et du stade précédent voire du suivant, pour affiner et valider la solution fournie, en fonction des décisions du CODIR.

Les activités doivent être adaptées à minima, en fonction de la taille et la complexité du projet.

2.1. **Objectifs.**

Disposer d'un système techniquement éprouvé et homologué, qui respecte les choix du stade précédent.

Rendre opérationnelles les interactions entre le SIC réalisé au stade précédent et son environnement (hommes et machines).

Itérations successives de 5 phases : conception, réalisation, vérification, intégration et mise à disposition.

2.2. **Déclenchement de l'entrée dans le stade.**

Sortie du stade d'études, ou GTEP/GIS-J5 en cas d'affermissement de tranche conditionnelle (TC).

Contractualisation interne ou notification d'un marché effectuée.

2.3. **Activités.**

Passer en GTEP/GIS-J3, si l'élément déclencheur n'est pas déjà un GTEP/GIS-J5.

Phase de conception des plans précis du SIC :

- concevoir le SIC (spécifications détaillées techniques et fonctionnelles) ;
- domaine SSI (démarche non simplifiée) :
    - valider le PDS et le POD définitifs ;
- finaliser la conception des tests (plans, jeux, environnement, outils) ;
- fiabiliser les données existantes à reprendre.

Phase de réalisation du SIC :

- réaliser le SIC (paramétrage/développement) ;

- enrôler le SI au centre technique de lutte informatique défensive (CTLID) ou au centre d'analyse en lutte informatique défensive (CALID) ;

- définir les procédures d'installation, d'exploitation, d'administration, d'exploitation de la sécurité et de continuité/reprise informatique ;

- rédiger les manuels (installation, exploitation, administration, utilisateurs) ;

- préparer le déploiement (y compris la conduite du changement) ;

- préparer la formation des utilisateurs et la conduite du changement ;

- finaliser le contrat d'opération (cf. annexe IV.) ;

- finaliser les modalités d'intégration (cf. annexe IV.) ;

- préparer le contrat de service (cf. annexe IV.).

Phase de vérification du SIC :

- effectuer les tests de « recette usine ».

Autorisation obligatoire par le CODIR de lancer l'enrôlement du SIC, au vu notamment de la décision d'homologation de référence, pour passer aux activités suivantes.

Phase d'intégration :

- préparer et organiser la mise en production du SIC ;

- mettre en place l'environnement d'exploitation et d'administration (cf. annexe IV.) ;

- installer le SIC sur les infrastructures d'hébergement ;

- paramétrer ;

- effectuer une VABF ;

- finaliser le contrat de service (cf. annexe IV.) ;

- auditer (au sens SSI) ;

- préparer le dossier de sécurité ou le dossier d'homologation ;

phase de déploiement :

- migrer les données ;

- conduire le changement ;

- former et assister l'ensemble des utilisateurs ;

- mettre en place l'organisation de support ;

- effectuer une VSR ;

- mettre en œuvre le contrat de service (cf. annexe IV.) ;

- effectuer un bilan du projet, puis passer en GTEP/GIS-J4.

2.4. **Éléments produits intermédiaires et/ou de sortie (suivant le plan de management).**

PM mis à jour.

PV de « recette usine », PV de VABF, de VSR.

Manuels (installation, exploitation, administration, utilisateurs).

Décision d'homologation de déploiement.

Plan de déploiement.

Plan et documents de formation.

Plan de communication.

Documentation sur le SIC.

Plan de tests SSI, plan de continuité informatique (PCI).

Procédures d'exploitation de la sécurité (PES).

Décision d'homologation de référence du SI ou autorisation provisoire d'exploitation.

SIC opérationnel, accessible à l'ensemble des utilisateurs.

Bilan [retour d'expérience (RETEX)] du projet.

Contrat de service (cf. annexe IV.).

2.5. **Déclenchement de sortie du stade.**

Décision formelle de mise en service opérationnel (MSO) prononcée par le CODIR.

3. STADE D'UTILISATION.

La responsabilité de ce stade incombe au RF du système. Ce stade ne concerne que la version en exploitation et ne présage pas du lancement d'une évolution majeure, qui ce traitera en parallèle en mode projet.

3.1. **Objectifs.**

Assurer la permanence de l'opérationnalité du SIC tout en maintenant son niveau de sécurité.

3.2. **Déclenchement de l'entrée dans le stade.**

Sortie du stade de déploiement.

3.3. **Activités.**

Exploiter les fiches d'incidents transmises par les structures de soutien.

Spécifier et réaliser (ou faire réaliser) le MCO hors évolutions majeures.

Réaliser (ou faire réaliser le MCS).

Mettre en place des indicateurs pour mesurer la satisfaction des utilisateurs.

Tenir à jour le dossier de sécurité du SIC.

Tenir à jour les données de coût global.

Aider à l'anticipation du retrait de service.

Passer en GTEP/GIS-J5 pour revue annuelle et/ou de renouvellement de contrat de MCO.

3.4. **Éléments de sortie (suivant le plan de management).**

Fiches de faits techniques.

Tableaux de bord (indicateurs).

Enquêtes de satisfaction.

Décisions de maintien de l'homologation.

3.5. **Déclenchement de sortie du stade.**

Enclenchement du processus de retrait de service, sur demande de l'AC ou du (des) RZF.

- éléments nécessaires à l'émission de la demande : pré-études issues de projets ou de processus externes.

4. STADE DE RETRAIT DE SERVICE.

La responsabilité de ce stade incombe au RZF.

4.1. **Objectif.**

Limiter les impacts négatifs consécutifs à l'arrêt définitif d'exploitation du SIC.

4.2. **Déclenchement de l'entrée dans le stade.**

Sortie du stade d'utilisation.

Accord conjoint de l'AC et du (des) RZF.

4.3. **Activités.**

Phase d'analyse :

- réaliser une analyse de risques ;

- élaborer un planning de retrait de service du SIC ;

- identifier les ressources et l'organisation à mettre en place pour le retrait ;

- élaborer un plan d'accompagnement ;

- enclenchement des activités de retrait effectif de service sur validation du GTEP/GIS-J6 au vu des modalités de retrait de service du système qui lui sont présentées.

Phase de retrait effectif :

- informer les utilisateurs ;

- arrêter le service ;

- archiver (cf. annexe V.), détruire et/ou reprendre les données ;

- désinstaller le SIC.

4.4. **Éléments de sortie.**

PV de retrait de service.

4.5. **Déclenchement de sortie du stade.**

Enregistrement du retrait de service officiel par le RZF.

---

(1) Y compris ce qui en découle à cause de la réglementation.

ANNEXE IV.
ENRÔLEMENT.

Le RCP doit préparer l'enrôlement du SI durant les deux premiers stades du projet pour garantir que le SI répondra de manière satisfaisante et durable aux objectifs fixés.

La demande est initiée par le RCP dès la phase d'initialisation du stade d'études afin que l'opérateur soit associé à la conduite du projet par la nomination du CAT.

Dès que cela est possible, une expression de besoin en hébergement est rédigée. Ce document comprend les éléments d'architectures technique et applicative ainsi que le niveau d'hébergement souhaité. Ces éléments permettent alors à la mission capacitaire de dimensionner les ressources nécessaires sur les structures d'hébergement, de définir un niveau d'hébergement en fonction de la maîtrise par l'opérateur de la pile logicielle du système et de proposer un lieu d'hébergement. Les équipes d'exploitation du futur centre d'hébergement peuvent alors travailler, avec le concours du CAT, à la préparation des opérations d'enrôlement proprement dites. Ces opérations doivent être planifiées et contractualisées avec l'opérateur au travers d'un contrat d'opération puis d'un contrat de service.

1. LE CONTRAT D'OPÉRATION.

Le contrat d'opération décrit les opérations qui devront être réalisés par l'opérateur et par la direction de projet dans le cadre de la procédure d'enrôlement jusqu'à la MSO du SI.

Ce document est susceptible d'être modifié au cours des comités de pilotage du projet.

Il comprend *a minima* les exigences de livraison de la documentation décrivant les architectures technique, applicative et des flux du SI ainsi que la documentation indispensable à l'installation et à l'exploitation du SI par les équipes de mise en d'œuvre.

Le bénéficiaire y indique ses souhaits de réactivité de la part des équipes de l'opérateur dans les phases préalables à la MSO, donc avant la mise en place du contrat de service. Il précise les dates prévisionnelles de livraison du système à intégrer et des activités de tests. En cas de décalage de livraison ou de non-tenue du nouveau système aux tests, cette étape d'intégration est renégociée avec l'opérateur en fonction de la disponibilité de ses équipes.

2. L'INTÉGRATION DU SYSTÈME D'INFORMATION.

Vue de l'opérateur, l'intégration d'un SI au sein de l'environnement du ministère de la défense comprend les phases :

- d'installation du système (ou d'une évolution) sur l'environnement d'intégration, conformément à la documentation d'installation livrée par l'équipe de réalisation (RRP) ;

- de recette fonctionnelle conformément à un cahier de tests validé par le RF du projet, et joué par des acteurs fonctionnels ;

- d'installation du système sur l'environnement de pré-production, environnement en tout point identique à l'environnement de production mais inaccessible par les utilisateurs (cet environnement peut être temporaire pour des raisons de gestion de la capacité, à la charge de l'opérateur) ;

- de test de montée en charge, permettant de valider que l'architecture du système répond bien aux estimations en terme de temps de réponse aux requêtes utilisateurs, de traitement des batchs et de nombre d'utilisateurs maximum et simultanés ;

- d'installation du système sur l'environnement de production.

En cas de difficulté lors de la phase d'intégration, les responsables techniques, fonctionnels ou de conduite du projet peuvent demander un test de qualité du code, suivant la criticité et les difficultés rencontrées.

3. LE DÉPLOIEMENT DU SYSTÈME D'INFORMATION.

La complexité du déploiement du système dépend de son architecture et de l'hétérogénéité de la population de ses utilisateurs. Plus la cible de déploiement finale est complexe et importante, plus il est important de prévoir un déploiement incrémental d'une part, et des tests de montée en charge d'autre part.

Le déploiement de tout client lourd est à la charge de l'opérateur, sur la base d'un calendrier de déploiement validé en CODIR projet, et à partir de master (déploiement manuel) ou d'un package (déploiement par télédistribution) fourni par le RRP.

Attention : pour les déploiements en outre-mer et à l'étranger (OME), qu'il s'agisse d'installation de client lourd sur des postes ou de la simple utilisation de réseaux de communication depuis ou vers ces derniers, les services et instances de l'opérateur en charge de l'OME doivent être consultés et doivent donner leur accord ; ceci afin de prendre en compte les impacts possibles sur les moyens dédiés principalement aux opérations extérieures.

Dans la mesure du possible, pour un SI déployé à l'outre-mer, l'utilisation de la bande passante de connexion d'un poste client avec les serveurs doit être optimisée. Le cahier des charges du projet peut fixer une limite haute à ne pas dépasser afin de maîtriser l'utilisation des réseaux. Une cartographie de l'utilisation des réseaux en fonction des sites (bande passante par client multipliée par le nombre de clients) devra être fournie afin de déterminer l'impact du SI sur les réseaux OME et si nécessaire un devis.

4. LE CONTRAT DE SERVICE.

À l'issue des étapes de mise en production et de déploiement, et avec le retour d'expérience de la VSR, l'opérateur est en mesure de proposer un contrat de service à la direction de projet.

En effet, la période de VSR doit permettre à l'opérateur de mesurer le niveau de service et la garantie de temps de rétablissement qu'il peut effectivement assurer sur le nouveau SI en production, notamment avec la mise en place d'une supervision technique et applicative ainsi qu'avec l'utilisation des documentations relatives à la PES. Le contrat de service est la formalisation écrite des engagements de l'opérateur à assurer les tâches qui lui incombent dans les délais négociés et en retour, des engagements de la direction de projet à fournir les correctifs et les documentations associées pour permettre l'exploitation du SI dans les meilleures conditions possibles.

Le contrat de service permet de définir, suivant le niveau d'hébergement assuré par l'opérateur et pour chaque élément de la pile logicielle et chaque opération d'exploitation et/ou d'administration à réaliser sur cet élément, l'acteur responsable de cette opération au travers de sa matrice des responsabilités. Il est possible, suivant certaines conditions liées à la pile logicielle du SI notamment, que tout ou partie de l'exploitation du système soit confiée à une tierce maintenance d'exploitation (TME). Le contrat de service doit indiquer dans ce cas les différentes responsabilités externes.

Enfin, le contrat de service précise les éléments de la chaîne de soutien du SI, les acteurs (et leurs coordonnées) du centre de service et des chaînes techniques et fonctionnelles qui sont amenées à intervenir sur le SI pour garantir le temps de rétablissement contractualisé.

ANNEXE V.

ADMINISTRATION DE DONNÉES.

1. ENJEUX DE L'ADMINISTRATION DES DONNÉES.

La qualité des données a un impact majeur le service rendu par les SI ; elle conditionne aussi l'interopérabilité des SIC, et la migration de données lors de la refonte des SIC.

Garantir la qualité des données relève de la démarche de gouvernance des données du ministère, démarche dont l'administration des données (ADD) constitue un pan majeur.

2. MISE EN ŒUVRE DE LA DÉMARCHE D'ADMINISTRATION DES DONNÉES AU MINISTÈRE DE LA DÉFENSE.

La directive n° 14/DEF/DGSIC du 19 juillet 2010 portant sur l'administration des données du ministère de la défense, fixe les règles permettant la mise en œuvre de la démarche pour l'ensemble des SIC du ministère, en concentrant les efforts de l'administration sur les données transverses (1) au SI et en calquant les responsabilités liées aux données sur celles de la démarche d'urbanisation. Au titre de l'ADD, les données transverses sont décrites, notamment sur proposition des projets, puis publiées sur un registre documentaire ministériel afin d'être utilisées dans les projets de SI et d'assurer à terme une cohérence d'ensemble. Leurs descriptions portent sur la sémantique de la donnée, sa représentation (format, etc.) et la définition de ses valeurs de référence le cas échéant ; elles sont réalisées sous la forme d'un modèle conceptuel de données dit modèle de données transverses de zone fonctionnelle (MDT-ZF).

Afin de mettre en œuvre les processus concourants à cette démarche, les acteurs, en termes de rôles, ont été identifiés :

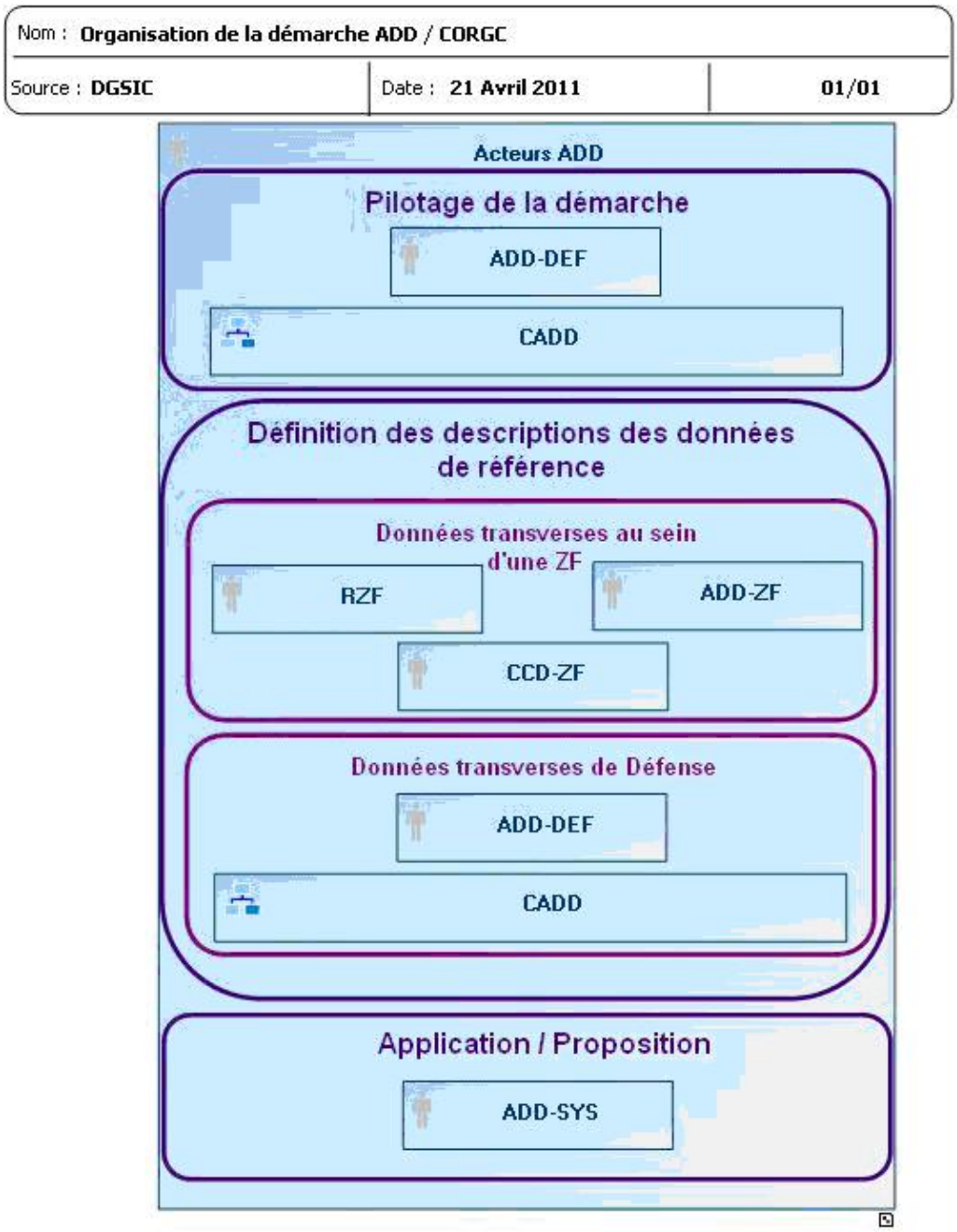
- l'administrateur des données Défense (ADD-DEF) : il pilote la démarche en concertation avec le centre des administrateurs de données (CADD) et est responsable du processus de définition des données lorsque celles-ci sont utilisées au sein de plusieurs ZF ;

- le RZF : il est le propriétaire des données de sa zone et est responsable de la mise en œuvre de la démarche au sein de celle-ci. Il désigne, à ce titre, un administrateur de données de zone fonctionnelle (ADD-ZF) et valide les descriptions des données de référence ;

- l'ADD-ZF : par délégation du RZF, il assure la description des données de référence de sa zone fonctionnelle en coordination avec les experts métiers de son domaine, rassemblés en comité de cohérence de données de zone fonctionnelle (CCD-ZF) ;

- ADD-SYS : il est désigné par le RF du projet et est le garant du respect de la démarche dans les projets. Il applique la démarche d'ADD au projet et est force de proposition sur les données à décrire en tant que données de référence ;

- le CADD est constitué de l'ADD-DEF et des ADD-ZF. Outre sa contribution au pilotage, il intervient lors de la validation des descriptions de données de référence transverses à plusieurs ZF.



3. L'ADMINISTRATION DES DONNÉES AU SEIN D'UN PROJET.

Le RF du projet doit nommer, dès le démarrage du projet, l'ADD-SYS au sein de l'équipe de projet. Celui-ci aura à sa charge :

- la déclinaison des exigences de l'ADD en termes de réutilisation des descriptions des données de référence au sein du projet et de définition des livrables dédiés à l'ADD. Ces exigences sont inscrites dans le cahier des clauses techniques particulières (CCTP), dans le cadre d'une externalisation, ou bien dans le PM ;

- l'identification des données de référence à prendre en compte dans le projet, à partir de l'expression de besoin en données, et ceci en interaction avec le ou les ADD-ZF des ZF impactées par le projet, ou l'ADD-DEF le cas échéant ;

- la gestion des dérogations à la directive, le cas échéant ;

- la vérification de la conformité des livrables de l'ADD ;

- la soumission de la description des données du système incluant :

  - la proposition de nouvelles descriptions de données de référence pour les données du système identifiées comme transverses et ne faisant pas déjà l'objet d'une description de référence ;

  - la publication des données du système sous forme d'un modèle de données du système (MDD-SYS), réalisé à partir des livrables de l'ADD et ceci en conformité avec les principes et les outils ministériels (AGL MEGA étendu METCAM/ADD). Ce modèle est publié sur le registre documentaire ministériel ;

- la participation à la mesure de la performance de la démarche d'ADD par le biais d'un bilan de la démarche ADD au sein du projet.

Tout au long de la vie du SI, les avancées de l'ADD doivent figurer dans la fiche observatoire des systèmes d'information et communication (OSIC) conformément au guide de rédaction de cette fiche.

4. CONTACT.

Pour toute information relative à la démarche d'ADD, le contact est l'ADD-DEF, à la sous-direction de l'ingénierie des systèmes d'information (SDISI) de la DGSIC.

---

(1) Donnée transverse : donnée échangée ou partagée.

ANNEXE VI.

OBLIGATIONS VIS-À-VIS DE LA COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS.

L'instruction n° 954/DEF/SGA du 13 septembre 1994 concernant l'application au ministère de la défense des dispositions de la 1oi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

La loi n° 78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés stipule que « l'informatique ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».

Aucun « traitement » « d'informations nominatives ou indirectement nominatives et *a fortiori* un traitement faisant appel à des techniques pouvant porter atteinte aux libertés et à la vie privée ou collectant des « données sensibles » ne soit mis en service, même à titre expérimental, sans qu'il ait été soumis à la CNIL, autorité administrative indépendante chargée de veiller au respect des dispositions de la loi précitée. Cette autorité dispose d'un pouvoir réglementaire dans le cadre prévu par la loi. ».

1. LES RÈGLES DE BASE.

Sont réputées nominatives, au sens de la loi n° 78-17 du 6 janvier 1978 modifié, les informations (y compris les photographies) qui permettent sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent.

La simple collecte est considérée comme un traitement.

Par « données sensibles » il faut entendre les données nominatives qui, directement ou indirectement, font apparaître l'origine raciale, les opinions politiques, les convictions philosophiques, religieuses ou autres convictions, les appartenances syndicales ou les mœurs des personnes ainsi que les données personnelles relatives à la santé ou à la vie sexuelle.

Il faut d'ailleurs indiquer dans les écrans et la documentation des applications que toute personne dispose d'un droit d'accès et de rectification des informations qui la concernent, qu'elle a le droit de connaître et de contester les informations et les raisonnements utilisés dans les traitements automatisés et dont les résultats lui sont opposés.

Au ministère de la défense des adaptations permettent de respecter la confidentialité de certains traitements. Ces traitements sont prévus par le décret n° 79-1160 du 28 décembre 1979 fixant les conditions d'application aux traitements d'informations nominatives intéressant la sûreté de l'État, la défense et la sécurité publique de la loi n° 78-17 du 6 janvier 1978.

2. LES ACTEURS DE LA COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS.

2.1. **Le correspondant général du ministère de la défense.**

Pour faciliter les relations avec la CNIL, le SGA dispose d'un correspondant général par qui transitent systématiquement, à l'aller comme au retour, tous les dossiers de déclarations de traitements automatisés d'informations nominatives préparés par les états-majors, directions et services de la défense (y compris les organismes sous tutelle).

2.2. **Les correspondants particuliers et organismes.**

Chacun des organismes doit mettre en place un correspondant particulier, désigné par l'autorité dont il relève. Ce correspondant d'organisme est en charge du portefeuille des systèmes de son ressort. Il doit vérifier que tous les systèmes qui le doivent respectent la loi.

3. LES PROCÉDURES.

Tout traitement automatisé d'informations nominatives doit être déclaré :

- soit dans le cadre d'une procédure de demande d'avis préalable de la CNIL : les décisions de création de ces traitements doivent alors prendre obligatoirement la forme d'un acte réglementaire (décret ou arrêté ministériel) ;

- soit dans le cadre d'une procédure de déclaration simplifiée.

Il existait une procédure particulière de simple déclaration (appelée déclaration ordinaire) auprès de la CNIL pour les traitements mis en œuvre antérieurement au 1er novembre 1979. Ces dispositions ne sont plus applicables, les déclarations ordinaires étant réservées au « secteur privé ».

Selon la nature des données traitées, le périmètre du projet, les interconnexions possibles et la diffusion des informations, deux types de déclarations doivent être faites.

3.1. **Procédure de demande d'avis préalable.**

Utilisation du répertoire national d'identification des personnes physiques (RNIPP) c'est-à-dire une consultation occasionnelle ou systématique, automatisée ou non de ce répertoire, y compris le fait de mentionner dans un fichier le numéro d'inscription au répertoire (NIR) ou ses formes dérivées (numéro de sécurité sociale par exemple).

Certains organismes sont autorisés d'emblée par décret. Un arrêté ministériel visant le décret est suffisant pour utiliser le NIR ou consulter le RNIPP si la finalité du traitement implique sa collecte (paye, sécurité sociale, etc.).

Transmission d'informations nominatives entre le territoire français et l'étranger.

Mise en mémoire d'informations nominatives qui, directement ou indirectement font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales ou les mœurs des personnes. Dans ce cas, le décret exigé doit être pris sur avis conforme de la CNIL.

Le dossier de « demande d'avis », comprenant le formulaire adéquat, un projet d'arrêté et éventuellement un projet de décret accompagné d'un projet de rapport au Premier ministre, est préparé par le service déclarant. Il est établi en cinq exemplaires (un original et quatre copies).

Le dossier est transmis pour instruction et centralisation, au correspondant particulier de l'état-major ou de la direction dont relève le déclarant puis au correspondant ministériel.

La CNIL dispose d'un délai de deux mois pour faire connaître son avis (à la date du dépôt du dossier). À l'expiration du délai de deux mois l'avis de la CNIL est réputé favorable si elle ne s'est pas exprimée.

Ce n'est qu'après avis favorable de la CNIL que le ou les actes réglementaires créant les traitements visés sont signés par les autorités.

3.2. **Procédure simplifiée.**

Pour les catégories les plus courantes de traitements à caractère public ou privé, qui ne comportent manifestement pas d'atteinte à la vie privée ou aux libertés, la CNIL a établi des normes simplifiées. Le dossier a pour objet de rattacher le traitement à une norme par une déclaration simplifiée de conformité.

Cette déclaration ne peut concerner qu'un seul service mettant en œuvre le traitement.

La procédure à suivre est la suivante :

- préparation de la déclaration par le service déclarant (transmission du dossier par le RCP à son correspondant CNIL d'organisme) ;

- signature par l'autorité cliente qui aurait à présenter le dossier s'il était soumis à la procédure de demande d'avis ;

- transmission du dossier au correspondant général du ministère de la défense qui dépose, après instruction, le dossier directement à la CNIL contre reçu.

La CNIL instruit le dossier et produit un récépissé autorisant le traitement. Dès que le récépissé est parvenu au correspondant d'organisme, le traitement peut être mis en œuvre.