



Conforme à l'original produit;
Début du texte, page suivante



BULLETIN OFFICIEL DES ARMÉES



Édition Chronologique n° 22 du 7 juin 2018

PARTIE PERMANENTE
Administration Centrale

Texte 1

INSTRUCTION MINISTÉRIELLE N° 2007/DEF/DGSIC

relative au pilotage d'un système d'information outillant les processus de fonctionnement du ministère, pendant tout le cycle de vie jusqu'au retrait de service.

Du 24 mars 2014

INSTRUCTION MINISTÉRIELLE N° 2007/DEF/DGSIC relative au pilotage d'un système d'information outillant les processus de fonctionnement du ministère, pendant tout le cycle de vie jusqu'au retrait de service.

Du 24 mars 2014

NOR D E F E 1 4 5 2 6 4 6 J

Texte abrogé :

Instruction n° 2007/DEF/DGSIC du 30 septembre 2011 (BOC N° 51 du 9 décembre 2011, texte 1 ; BOEM 160.6.2) modifiée.

Classement dans l'édition méthodique : BOEM 160.3

Référence de publication : BOC n° 22 du 7 juin 2018, texte 1.

SOMMAIRE

1. OBJECTIFS ET DOMAINE D'APPLICATION.

2. ACTIVITÉS PRINCIPALES.

2.1. Les activités menées avant la réalisation.

2.2. Les activités menées dans le cadre de la réalisation d'un système d'information.

2.3. Les activités menées dans le cadre de l'utilisation du système d'information.

2.4. Les activités menées dans le cadre du retrait de service.

3. RÔLES ET RESPONSABILITÉS.

3.1. Gouvernance générale.

3.2. En conduite de projet (jusqu'à l'entrée en phase d'utilisation).

3.3. Au passage en phase d'utilisation du système d'information.

3.4. Instances de décision et d'examen.

3.5. Opérateur.

3.6. Sécurité des systèmes d'information.

3.7. Contrôle financier.

3.8. Contrôle de la capacité de développement interne.

3.9. Dispositions particulières pour les urgences opérationnelles.

4. CONDUITE DES PROJETS.

4.1. Démarche détaillée.

4.2. Plan de management de projet.

4.3. Exigences réglementaires.

4.4. Livrables obligatoires.

5. DIVERS.

ANNEXE(S)

ANNEXE I. GLOSSAIRE.

ANNEXE II. COHÉRENCE DES PHASES ET DES JALONS.

ANNEXE III. ENRÔLEMENT.

ANNEXE IV. ADMINISTRATION DE DONNÉES.

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

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 maintenir un système d'information (SI) ⁽¹⁾, sans préjuger de la distribution de ces rôles dans l'organisation du ministère.

La présente instruction définit le processus de conduite d'un SI ainsi que les rôles correspondants à tenir que ce soit pour :

- aboutir à la conception du SI, après validation de l'expression initiale du besoin au jalon 0, jusqu'à la fin de la réalisation ;
- traiter les évolutions majeures (évolutions du périmètre fonctionnel, refonte technique...) susceptibles de réactiver une équipe projet ;
- gérer l'utilisation courante du SI et son retrait de service.

Nota bene : pendant l'utilisation du SI, une version N peut être en service, tandis qu'une version N +1 (évolution majeure) peut être en projet (études et/ou réalisation). Ainsi des versions successives d'un SI peuvent coexister à des phases différentes de son cycle de vie.

Elle indique les activités à conduire et les résultats attendus, en cohérence avec les modalités d'approbation et de suivi à effectuer qui relèvent d'une autre instruction ⁽²⁾. Certaines activités peuvent être regroupées et/ou développées en fonction de la complexité du projet.

Cette instruction fixe le cadre dans lequel doivent s'inscrire les méthodes de conduite de projet (méthodes agiles, PHARE, en V, ...)

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 de projet doit être établi et doit préciser l'attribution des responsabilités, l'organisation nécessaire mise en place, les éventuels compléments ou aménagements dans l'enchaînement des activités, et enfin les documents obligatoires qui devront être formalisés, en tenant compte de la complexité du projet pour se limiter à une juste suffisance. Il est néanmoins important que les rôles et responsabilités décrits au point 2 soient bien identifiés, un cumul de fonctions par une même personne restant possible.

Cette instruction s'applique aux SI outillant les processus de fonctionnement du ministère, en particulier les SI d'administration et gestion (SIAG). Son application à d'autres systèmes d'information ⁽³⁾ peut être envisagée selon l'orientation de l'entité qui en a la responsabilité.

2. ACTIVITÉS PRINCIPALES.

L'expression du besoin initial comprend la définition ou la révision de l'organisation du travail et des processus à outiller, sous la responsabilité des organismes métiers. Son processus de validation est traité dans une autre instruction ⁽⁴⁾.

La formalisation 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 les phases du projet, où « clients » et « fournisseurs » restent en liaison pour optimiser la solution élaborée.

Les différentes phases du cycle de vie du SI à conduire sont décrites en annexe.

2.1. Les activités menées avant la réalisation.

Ces activités correspondent aux phases d'initialisation, d'orientation et d'élaboration décrites dans l'IM 2008.

La phase d'initialisation est centrée sur l'élaboration de l'étude d'opportunité et de dans le but d'obtenir le feu vert de lancement de réalisation du SI en fin de phase (franchissement du jalon 1).

Cette phase couvre en particulier la mise en place des compétences et des équipes de conduite de projet, de réalisation et d'hébergement/exploitation 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 seront à détailler dans un plan de management de projet.

Les phases d'orientation et d'élaboration vont permettre d'une part de formaliser les exigences fonctionnelles et les contraintes, et d'autre part de contractualiser avec un prestataire externe (consultation, dépouillement des offres et choix du titulaire) ou avec un centre de développement interne (inscription au plan de réalisation). Elles se terminent au passage du J3.

2.2. Les activités menées dans le cadre de la réalisation d'un système d'information.

Ces activités correspondent à la phase de réalisation décrite dans l'IM 2008. Elles se concluent par la mise en production et le déploiement du SI réalisé (franchissement du jalon 4).

2.2.1. 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. Il est alors possible de procéder à la recette complète du système [notion de

vérification de service régulier (VSR)].

La conduite du changement, préparée lors des phases précédentes, doit être mise en œuvre lors de cette phase.

2.3. Les activités menées dans le cadre de l'utilisation du système d'information.

Ces activités correspondent à la phase d'utilisation décrite dans l'IM 2008.

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 préalable d'étude du nouveau besoin.

2.4. Les activités menées dans le cadre du retrait de service.

Ces activités correspondent à la phase de retrait de service décrite dans l'IM 2008.

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 autorités utilisatrices. Le sort réservé aux données générées par le SI a été défini via la stratégie d'archivage des contenus du système d'information au cours de la phase d'orientation du projet ⁽⁵⁾.

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...).

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

Dès la phase préalable d'étude du besoin, l'AC désigne un responsable fonctionnel RF qui portera le besoin pendant toute la vie du SI jusqu'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 responsable fonctionnel (RF), les conditions de mise en œuvre du SI et les objectifs de sécurité (modes de travail, processus, articulation avec d'autres métiers...) de leur responsabilité.

Les AU sont présentes ou représentées au comité directeur (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 (POS) du ministère qui leur est confié.

Les RZF et les RQF rédigent et entretiennent les schémas directeurs SIC (volets opérationnels) de leur zone ou quartier. 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 responsables des processus des AC. 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.

Le RZF ou RQF peut avoir délégation de l'autorité cliente pour la représenter.

3.1.4. Responsable système d'information et de communication d'organisme.

Le principal rôle du responsable SIC d'organisme est d'être le coordonnateur des besoins opérationnels et le garant de la cohérence des SIC utilisés par son organisme. Par organisme, on entend les armées, états-majors, directions et services.

Le RSIC peut avoir délégation de l'autorité cliente pour la représenter.

Quand le projet est pris en charge par son organisme que ce soit pour ses propres besoins en tant qu'AU ou pour toute autre AU du ministère, il peut être désigné par l'AC pour veiller à la cohérence d'ensemble sur le plan organique.

3.1.5. 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 participe aux revues et examens des principaux projets et au besoin, mène des audits.

3.1.6. Direction interministérielle des systèmes d'information et de communication.

La direction interministérielle des systèmes d'information et de communication (DISIC) 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.

3.2. En conduite de projet (jusqu'à l'entrée en phase d'utilisation).

3.2.1. Responsable fonctionnel du projet.

Le responsable fonction (RF) du projet porte le besoin fonctionnel pendant tout le cycle de vie du SI. Il représente ce que l'on appelle couramment la maîtrise d'ouvrage (MOA). Le RF est un spécialiste de son domaine métier, en mesure de concevoir l'évolution des processus concernés. Dans le cadre du projet, il est fonctionnellement rattaché à l'autorité cliente.

Le RF 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 est responsable de l'étude d'opportunité, de la description des gains obtenus sur le fonctionnement et l'efficacité de ses processus métiers, et de la justification du retour sur investissement. Il rédige le cahier des charges fonctionnel et exprime les priorités. Il définit les cibles de déploiement ainsi que les performances attendues, qui seront validées par l'AC.

Le RF est responsable et pilote de la conduite du changement, de la formation (définition et organisation), du déploiement (sous l'angle métier), de la stratégie de reprise des données et de l'assistance aux utilisateurs. Il est responsable de la recette fonctionnelle de l'application développée, à ce titre il organise et conduit les tests fonctionnels. En liaison avec le responsable de conduite du projet (RCP), il doit garantir la qualité des données (reprises, gérées et produites par le SI).

Le RF préside le comité des utilisateurs.

Sa responsabilité persiste pendant la phase d'utilisation.

3.2.2. Responsable de conduite de projet.

Le responsable de conduite de projet (RCP) doit être un professionnel ⁽⁶⁾ de la conduite de projet. Il est responsable de l'atteinte des objectifs fixés tant dans les délais qui lui sont fixés que dans l'emploi les ressources, il rend compte au CODIR (présidé par l'AC) de l'avancée du projet en termes de coûts, délais et performances. Il met en œuvre les décisions concernant le projet et entretient leur historique et les justificatifs qui s'y rapportent. Il garantit la cohérence d'ensemble des documents produits et des actions réalisées.

Le RCP traduit ou fait traduire le besoin en spécifications fonctionnelles générales et détaillées, ainsi qu'en spécifications techniques. Il précise les ressources humaines et financières nécessaires à la conduite et la réalisation du projet. Il établit le devis du projet et assiste le RF dans l'analyse de la valeur du projet dans le but de justifier le retour sur investissement. Il assure le suivi financier du projet.

Le RCP est responsable de la création et de la mise à jour de la fiche dans l'outil ministériel de suivi du portefeuille (fiche SICL@DE).

Le RCP est garant de l'application des directives ministérielles ⁽⁷⁾ qui s'appliquent au périmètre du projet.

Le RCP établit et entretient le calendrier opérationnel du projet. Il en suit le tableau de bord et alerte sur les dérives. Il identifie et gère les risques du projet. Il supervise et coordonne l'ensemble des activités du projet, notamment le suivi des prestations du réalisateur et de l'hébergeur. Il rédige, en tant que prescripteur, les documents nécessaires à toute consultation en lien étroit avec l'acheteur. Il gère ⁽⁸⁾ la relation contractuelle avec le ou les prestataires intervenant sur le projet et réceptionne les prestations réalisées, y compris les livrables de conduite du projet.

Le RCP préside le comité de pilotage (COPIL) projet.

Le RCP est le correspondant de la maîtrise d'œuvre (MOE), représentée par le responsable de réalisation du projet (RRP).

Le RCP est responsable de l'emploi des compétences au sein de l'équipe de projet. Il pourra s'appuyer sur une équipe de conduite de projet intégrée (ECPI) composée pour la circonstance. Il devra alors évaluer les compétences qui lui seront nécessaires et en demander la mise à disposition aux différentes autorités d'emplois.

Le RCP s'appuie sur le ou les RSIC pour déployer le SI au sein du ou des organismes.

La présente instruction ne définit pas la façon dont les RCP sont organisés au sein du ministère ni leur rattachement organique. Il est cependant recommandé qu'ils puissent bénéficier d'un environnement où ils pourront trouver à la fois l'encadrement nécessaire et les ressources transverses dont ils ont besoin pour leur projet.

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

Un projet d'ensemble rassemble plusieurs projets, ou des projets et des systèmes déjà en production concomitants ou successifs concourant à la satisfaction d'un besoin complexe. Dans ce cadre :

- un responsable fonctionnel d'ensemble (RFE) est désigné pour assurer la cohérence fonctionnelle entre différents projets ou entre projets et systèmes déjà en production. Les avis et arbitrages sont émis au cours d'un Comité d'Orientation Fonctionnel (COF) ;
- un responsable de conduite de projet d'ensemble (RCPE) est désigné pour assurer la cohérence technique, calendaire et financière des différents projets, ou entre projets et systèmes déjà en production ;
- RFE et RCPE ont autorité de coordination sur les RF et RCP correspondants ; ils analysent les choix effectués par les projets, identifient les écarts entre les différents projets, ou entre projets et systèmes déjà en production, analysent leurs impacts, et proposent des actions à mettre en œuvre. Ils rendent compte aux CODIR des différents projets de la coordination entre projets et systèmes en production.

L'organisation et le financement mis en place pour chaque projet d'ensemble font l'objet d'une décision de la commission du segment concerné (9).

3.2.4. Responsable de réalisation du projet.

Le responsable de réalisation du projet (RRP) est un professionnel (10) du pilotage de la réalisation d'un SI. Il est responsable du développement, de l'intégration et du déploiement technique du SI en projet.

Une maîtrise d'œuvre (MOE) - interne ou externe - assure la réalisation du SI, suivant les règles en vigueur et les spécifications fonctionnelles et techniques définies par le RCP, dans le respect des directives et guides ministériels. 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. Le RRP constitue la MOE. 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 participe à la mise en place des moyens du déploiement, en coordination avec l'hébergeur.

Le RRP est responsable de la fourniture de la documentation technique du projet.

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. Elle perdure jusqu'à la fin de la phase de réalisation de la mise en service opérationnelle (MSO).

L'équipe de conduite de projet intégrée (ECPI), plus communément appelée équipe de projet, 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 représentés les rôles :

- d'architecte de système d'information (ASI) : il est responsable de la définition, de l'architecture du système au regard des directives ministérielles et de la validation des livrables afférents ;
- de responsable de sécurité des systèmes d'information projet (11) (RSSI-P) : un RSSI-P est désigné (12) pour piloter la démarche d'intégration de la SSI durant les deux premières phases, jusqu'à l'homologation initiale incluse, qu'il est chargé d'instruire (13). C'est donc lui qui prépare et conduit le processus d'homologation. Il assure également la phase de transfert de responsabilité vers le RSSI-Aval 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 GT SSI ad hoc instauré dès la phase d'orientation. Il est

responsable de la validation des livrables afférents ;

- d'acheteur (représentant du pouvoir adjudicateur dans le cas de prestations externalisées) ;
- de responsable de la reprise des données, il définit la stratégie de reprise des données à la création du SI et la stratégie d'archivage au long du cycle de vie, il est responsable de la validation des livrables afférents à la reprise des données. Il est aidé par un administrateur des données (ADD-SYS, administrateur des données système) (cf. annexe 4) responsable notamment de leur qualité ;
- de coordonnateur des activités techniques (CAT) : il traite des points relatifs à l'hébergement, à l'exploitation, aux réseaux, aux servitudes, etc. et valide les livrables afférents. Les responsabilités du CAT sont détaillées dans l'annexe traitant de l'enrôlement.

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

Les membres de l'équipe de projet partagent toutes les informations et proposent des décisions de façon conjointe, sous l'autorité du RCP.

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.

L'équipe de projet peut s'appuyer 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 de projet.

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 la documentation utilisateurs (en ligne ou hors ligne) et la formation,
- de préciser le besoin fonctionnel et de sécurité autant que de besoin,
- de définir l'évolution des compétences métier qui seront nécessaires pour mettre en service le SI,
- de faire remonter en COPIL, COF et/ou CODIR l'incidence sur les métiers des évolutions fonctionnelles et des arbitrages de la conduite du projet,
- de proposer au COPIL et/ou COF 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,

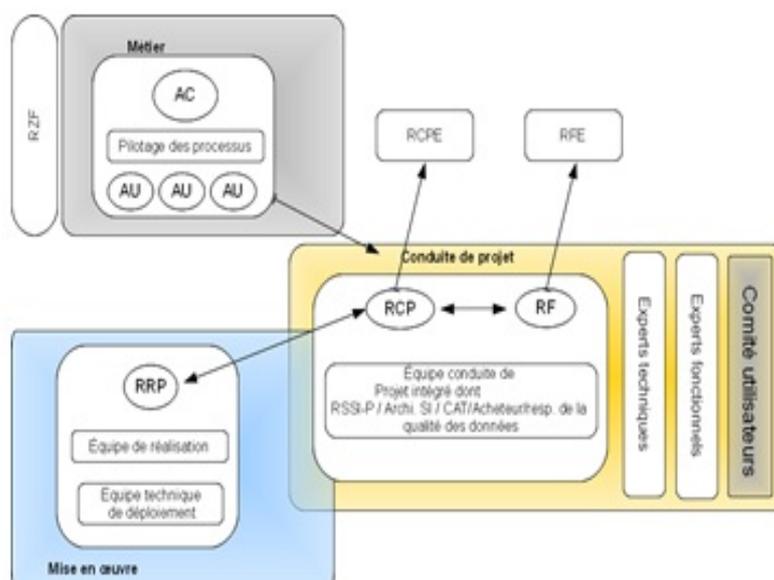
- de préparer et animer la conduite du changement.

3.2.7. Responsabilité de déploiement.

Le RCP traduit en exigences fonctionnelles et techniques les besoins du SI en matière de performance, de reprise d'activité, etc. Ces besoins sont validés in fine par les instances de gouvernance ad hoc du ministère [telles que le CODIR des Intranets qui comprend notamment l'autorité de régulation des réseaux (ARR)] (14). En liaison avec la MOE, l'ASI définit l'architecture du système, en tenant compte en particulier des spécifications techniques requises données par le CAT pour que le SI puisse être intégré au sein de l'architecture MINDEF (hébergement SHÉM, IGC, Annudéf, services STC-IA,...). Les besoins et l'architecture décrite sont étudiés avec l'hébergeur qui traduit ces éléments en livrables in fine validés par le CAT.

3.2.8. Articulation entre les acteurs de la conduite de projet.

Principaux rôles en mode « projet »



3.3. Au passage en phase d'utilisation du système d'information.

3.3.1. Responsable fonctionnel du système.

Le Responsable fonctionnel (RF) est de préférence le même qu'en phase de réalisation. 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 traitements des incidents de fonctionnement et 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 3.4.4). A ce titre, il instruit les demandes d'évolution (y compris le recensement d'un besoin d'évolutions majeures) et prépare les décisions du CODIR du système en exploitation, dont celles nécessitant un retour en mode projet.

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

Il organise les actions de formation d'adaptation nécessaires.

3.3.2. Responsable technique de système.

Responsable devant l'AC, le responsable technique de système (RTS) est responsable 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.

Il est aidé en cela par l'hébergeur et le responsable d'exploitation fonctionnelle.

3.3.3. Responsable d'exploitation fonctionnelle.

Le responsable d'exploitation fonctionnelle (RExpF) positionné au sein de l'AC, il assure l'exploitation fonctionnelle et la surveillance quotidiennes du système, ainsi que la gestion des incidents relatifs au fonctionnement du SI.

3.3.4. Responsable de la sécurité des système d'information aval et maintien en condition de sécurité.

Le responsable de la sécurité des système d'information aval (RSSI-A) 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.

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 (MCS).

3.3.5. Maintien en condition opérationnelle.

La fonction de MCO réalise les modifications applicatives du système en exploitation et de ses interfaces, qui relèvent de la phase 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.

Le MCO et le MCS sont fortement liés.

3.3.6. *Fonction d'exploitation.*

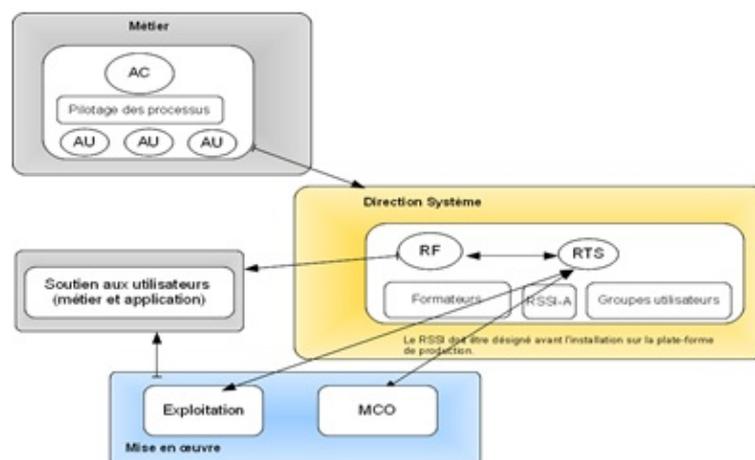
Cette fonction assure l'exploitation et la supervision quotidiennes du système, ainsi que la gestion des incidents et des changements, matériels ou logiciels, relatifs au fonctionnement du SI.

3.3.7. *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.

3.3.8. *Articulation des acteurs de la conduite de SI au stade d'utilisation.*

Principaux rôles en mode « utilisation du système »



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.

Le CODIR est chargé de superviser la conduite du projet, puis du système, et la réalisation de ses objectifs. Il valide le plan de management du projet. Il prend les décisions stratégiques instruites par l'équipe de conduite de projet et notamment l'affectation des moyens financiers, humains et matériels. Il procède aux arbitrages concernant le déroulement du projet dans son ensemble. Le CODIR oriente les mesures à prendre face aux risques. Il permet également d'assurer le partage et la transparence des informations entre les acteurs du ministère de la défense concernés par le projet ou le système.

Le CODIR est l'instance de décision associée au passage de jalons obligatoires, notamment la décision de déploiement et celle de mise en service opérationnel (MSO). Il 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.

Sur proposition du comité de gestion de configuration (cf. point 3.4.4), 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 (jusqu'à la phase de réalisation inclus) puis le RF du système (à partir de la phase d'utilisation) ;
- le RCP (jusqu'à la phase de réalisation inclus) puis le RTS du système (à partir de la phase d'utilisation) ;
- les représentants des structures de soutien concernées ;
- le représentant du pouvoir adjudicateur, le cas échéant ;
- le (ou les) RZF concerné(s), ou leurs représentants (RRZF) ;
- si le projet fait partie d'un projet d'ensemble, le RCPE et le RFE.

Le RF du projet puis système assure le secrétariat du CODIR (préparation, animation, compte rendu) en liaison étroite avec l'ensemble des membres, notamment le RCP ou le RTS.

La DGSIC, le responsable de budget opérationnel de programme (RBOP) concerné et la MSIAG (si le SI est de son périmètre) 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 comité de pilotage (COFIL) est mis en place pour assurer le pilotage et la conduite opérationnelle du projet.

Le COFIL du projet, présidé par le RCP, rassemble le RF du projet et l'ensemble de l'équipe projet, ainsi que les 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 COFIL, subordonné au CODIR :

- valide les décisions technico-fonctionnelles "courantes" proposées par l'équipe projet;
- prépare et 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 de projet ;
- s'assure et rend compte de la tenue des objectifs en termes de fonctionnalités – performances – coûts – délais – sécurité ;
- assure le suivi des risques sur le projet.

3.4.3. Comité d'orientation fonctionnelle.

Le comité d'orientation fonctionnelle (COF) est mis en place pour mener les travaux collaboratifs d'harmonisation fonctionnelle en phase de conduite de projets dans le cas d'un projet d'ensemble.

Il permet aux RFE et RCE :

- d'étudier et valider toute demande d'évolution fonctionnelle ;
- de proposer des leviers de convergence fonctionnelle et organisationnelle (simplification des processus, prérequis réglementaires, articulation des interfaces fonctionnelles, impacts sur les métiers ; etc.) ;
- d'analyser les risques métiers majeurs des projets entrant dans le périmètre concerné ;
- de préparer et proposer les décisions au CODIR.

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

- l'AC ou son représentant ;
- le RFE et le RCE ;
- les RF et RCP des projets et/ou des systèmes en production ;
- les AU ;
- le (ou les) RZF concerné(s).

Le RFE assure le secrétariat du COF (préparation, animation, relevé et suivi des décisions) en liaison étroite avec l'ensemble des membres, notamment le RCE.

3.4.4. 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 du point 3.3.8), 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 ;
- s'assure du pilotage du suivi des risques.

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

Tout SI doit être homologué par l'AQ désignée. Cette homologation est instruite par le RSSI-P ou le RSSI-A.

La commission d'homologation (CH) émet (conformément aux textes SSI en vigueur) un avis motivé sur la capacité du SI à traiter les informations protégées au niveau de sécurité requis. Mise en place à partir de la phase d'orientation, elle est garante du respect de la démarche d'homologation vis à vis de l'autorité d'homologation (AH). Elle prend des décisions au profit de l'AH en validant les différents passages de jalons SSI comme définis au sein de la stratégie d'homologation (SH) validée par l'AH.

3.4.6. Revues et examens.

Les modalités d'approbation et de suivi des systèmes d'information et de communication (SIC) des systèmes d'information et de communication sont définies par l'instruction n° 2008 DEF/DGSIC du 10 juillet 2013. Elle fixe en particulier les conditions de passage aux différents jalons (J0 à J6).

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 de la phase d'utilisation.

Sous la responsabilité du CAT, il doit être sollicité dès le démarrage du projet comme expert de l'exploitation et du soutien SIC de manière générale, au profit du projet, pour en préparer la phase 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 services communs, de pré-production et/ou de production.

À partir de la phase d'utilisation, après la MSO, le RTS assure la coordination avec l'opérateur pour faire réaliser les activités de MCO et/ou de MCS applicatif et matériel.

3.6. Sécurité des systèmes d'information.

La sécurité des systèmes d'information (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 principaux acteurs sont l'autorité qualifiée (AQ), l'autorité d'homologation (AH), et les RSSI-P et RSSI-A dont les rôles ont été définis précédemment.

Tout système doit être homologué ou obtenir une autorisation provisoire d'exploitation avant utilisation. L'homologation a pour objectif de garantir au travers d'une démarche structurée, précisée au sein de la stratégie d'homologation (SH) validée par l'AH, que les besoins de sécurité du système (fonctions implémentées et informations traitées) sont couverts par les mécanismes de sécurité natifs du SI ou par des mesures complémentaires techniques, de protection physique et organisationnelles devant être mises en œuvre par l'environnement d'accueil (ou de déploiement).

Le respect de ce processus s'effectue par la production à chaque étape du développement du SI de documents SSI dont la description détaillée est donnée au sein du Guide SSI Projet.

3.6.1. Autorité qualifiée.

L'autorité qualifiée (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'IGI 1300. 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 (AH) 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. Le responsable de budget opérationnel de programme.

Les responsables de budget opérationnel de programme (RBOP) vérifient la provision des ressources financières nécessaires aux projets puis aux systèmes en exploitation.

3.7.2. Comité ministériel d'investissements.

Suivant des seuils déterminés (50 M€ pour les SI hors opération d'armement), les dossiers de changement de phase aux différents jalons pour certains projets et les grandes décisions structurantes sont éventuellement proposés à l'ordre du jour du comité ministériel d'investissements (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).

Lorsqu'un projet est rattaché à une activité budgétaire réservée par la CEP et qu'il a fait l'objet d'une revue organisée par la MSIAG au titre de l'année en cours, la présidence de la CEP peut demander à se faire communiquer le rapport de revue.

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.

3.7.4. Direction interministérielle des systèmes d'information et de communication.

Selon l'article 7. du décret de création du DISIC ⁽¹⁵⁾, tout projet de SI de fonctionnement supérieur à 9 M euros doit obtenir l'accord formel du DISIC. Tout projet compris entre 5 et 9 M euros doit faire l'objet d'une information à la DISIC. Ces montants sont évalués selon les règles précisées par le DISIC (T2, T3 et T5).

3.8. Contrôle de la capacité de développement interne.

Le responsable ministériel du plan de réalisation interne vérifie la provision des ressources humaines de développement interne nécessaires aux projets puis aux systèmes en exploitation.

3.9. Dispositions particulières pour les urgences opérationnelles.

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 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.

4. CONDUITE DES PROJETS.

4.1. Démarche détaillée.

Les guides et méthodes de projets détaillent les activités à mener dans le cadre du cycle de vie des SI concernés par la présente instruction.

Les RCP se doivent d'utiliser ces guides et les méthodes éprouvées recommandées au sein du ministère. Ces guides et méthodes appuient le déroulé de la conduite de leurs projets, en fonction des enjeux et des risques de ceux-ci. Les plans de management de projet décrivent, entre autres, ce qui doit être formalisé.

4.2. Plan de management de projet.

Le plan de management de projet (PMP) est un document évolutif. Il est créé dès la phase d'initialisation (passage du jalon 1) et suit toutes les phases du projet. Il reste actif lors de la phase d'utilisation du système. Son rôle est d'être le document de référence sur l'ensemble du cycle de vie du système.

Le PMP 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 du projet,
- 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 PMP est complété en tant que de besoin

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

4.3. 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 (GIS et groupes de revues). L'instruction 2008 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 (n.i. BO)], mais aussi de l'opérateur (cf. annexe sur l'enrôlement des SI), de l'administration des données (cf. annexe correspondante), ou encore de la protection de la vie privée (cf. annexe sur la CNIL).

4.4. Livrables obligatoires.

Parmi la liste des livrables demandés dans le cadre strict de l'activité de conduite de projet de SI le long du cycle vie du projet puis du système, les éléments suivants requièrent une importance primordiale :

- Expression de besoin initiale ;
- Expression des objectifs de sécurité du système (FEROS) associés au besoin exprimé ;
- Analyse de la valeur et étude de retour sur investissement (application de la méthode MAREVA 2) ;
- Plan de management de projet (PMP) ;
- Evaluation de la charge RH et financière et leur suivi pendant toute la durée du projet ;
- Echancier en AE et CP ;
- Planning opérationnel de mise en œuvre du projet ;
- Cahier des charges fonctionnel (CdCF), qui peut être dans les cas très simples une reprise de l'expression de besoin initiale;
- DCE (dont le CCTP) et tous documents contractuels nécessaires dans le cas de MOE externe ;
- Rapport de présentation ;
- Acte d'engagement ;
- Portefeuille de risques ;
- Dossier d'architecture technique ;
- Dossier d'exigences couvertes avec matrice de traçabilité ;
- Documentation prévue dans le PMP, dont les documents techniques et utilisateurs ;
- Documentation SSI prévue à chaque étape dans le guide SSI projet, en particulier la PES ;
- Plan de reprise des données ;
- Stratégie et Plan de déploiement ;
- Plan de formation ;
- Plan de communication ;
- Stratégie d'archivage des données ;
- Besoins d'hébergement, d'exploitation et de supervision ;
- Besoins en infrastructure et servitudes (énergie, climatisation, sécurité passive, etc..) ;
- Besoin en MCO et MCS ;
- Besoins vis-à-vis des interfaces du système dont les réseaux (16) ;
- Le SI opérationnel (17) (avec codes sources documentés) ;

- Contrat de service avec l'hébergeur (cf. annexe 4) ;
- Procès-verbaux des recettes (usine, VA, VSR) ;
- Décision de mise en service opérationnelle (MSO) ;
- Comptes rendus formalisés des CODIR des COPIL et des COF ;
- Fiche SICLADE mise à jour ;
- Dossier de retrait de service ;
- PV de retrait de service (en fin de vie).

5. DIVERS.

La présente instruction abroge l'instruction n° 2007/DEF/DGSIC du 30 septembre 2011 relative au pilotage d'un système d'information outillant les processus de fonctionnement du ministère, de la conception au retrait de service.

Pour le ministre de la défense et par délégation :

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

Gérard LAPPREND.

-
- (1) Système d'information incluant les systèmes de communication et de transport d'information.
 - (2) IM 2008/DEF/DGSIC fixant les modalités d'approbation et de suivi des SIC
 - (3) SIOC hors opérations d'armement de l'EMA, SIC d'infrastructure développés et mis en œuvre par la DIRISI hors opérations d'armement, SIST de la DGA
 - (4) IM 2008/DEF//DGCIC fixant les modalités d'approbation et de suivi des SIC.
 - (5) directive n° 30 DEF/DGSIC du 5 décembre 2013
 - (6) C'est-à-dire qu'il doit avoir une bonne maîtrise dans ce domaine, en particulier dans les projets à fort enjeu.
 - (7) Directives techniques, achats, conduite, examens et suivi de projet, archivage des données, CNIL, etc.
 - (8) Dans le périmètre éventuellement fixé par le représentant du pouvoir adjudicateur (RPA)*
 - (9) CSIAG, CSIOC, CSIST

(10) C'est-à-dire qu'il faut avoir une bonne maîtrise dans ce domaine, en particulier dans les projets à fort enjeu.

(11) Parfois aussi appelé RSSI Amont.

(12) Si aucun RSSI-P n'est désigné, cette fonction essentielle est assurée par le RCP.

(13) En particulier, il conduit la rédaction de la FEROS* pour le ou les systèmes concernés.

(14) Autorité de régulation des réseaux

(15) Arrêté du 1er juin 2011 pris pour application de l'article 7 du décret n°2011-193 du 21 février 2011 portant création de la DISIC

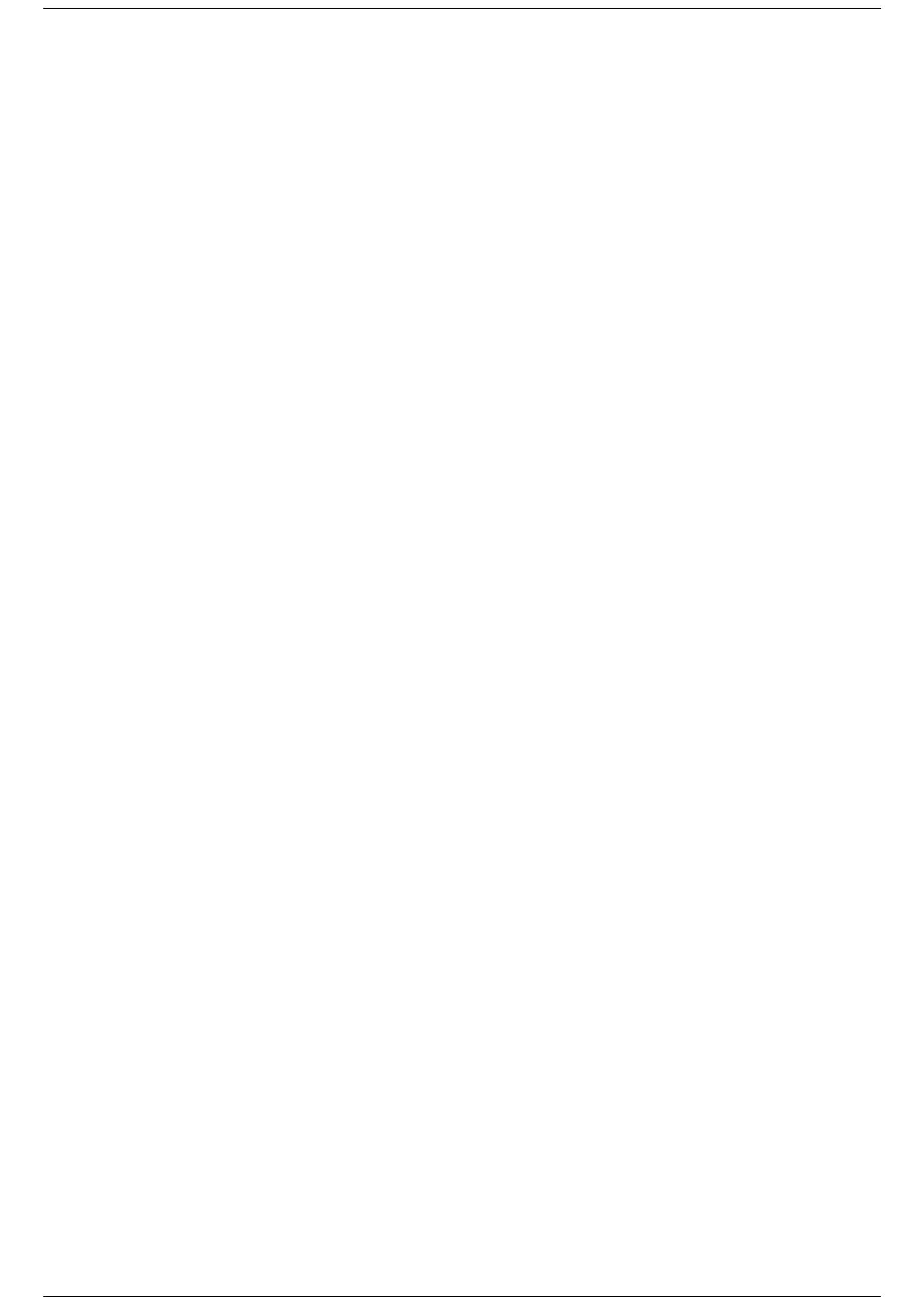
(16) Canevas des Applications en réseaux (CAR).

(17) C'est-à-dire l'objet du projet.

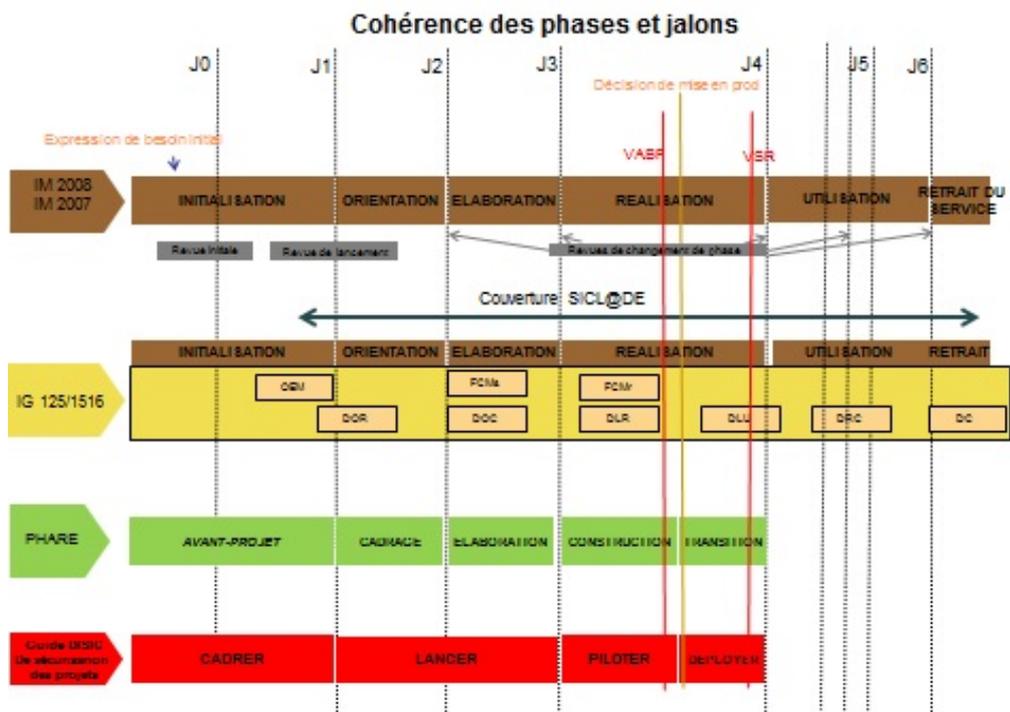
**ANNEXE I.
GLOSSAIRE.**

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
AE	Autorisation d'engagement
AH / AHP	Autorité d'homologation / Autorité d'homologation principale
Annudef	Annuaire de la Défense
AQ	Autorité qualifiée (SSI)
ASI	Architecte de système d'information
AU	Autorité utilisatrice
BOP	Budget opérationnel de programme
CALID	Centre d'analyse et de lutte informatique défensive
CAT	Coordonnateur es '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
COF	Comité d'orientation fonctionnelle
COPIL	Comité de pilotage
COVESIOC	Comité de convergence des SIOC
CP	Crédits de paiement
CSIC	Conseil des SIC
CTSIC	Commission technique des SIC
DAF	Direction des affaires financières
DCE	Document de consultation des entreprises
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

GIS	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
MOA	Maîtrise d'ouvrage
MOE	Maîtrise d'œuvre
MSIAG	Mission des systèmes d'information d'administration et de gestion
MSO	Mise en service opérationnel
OME	Outre-mer et à l'étranger
PCI	Plan de continuité informatique
PES	Procédures d'exploitation de la sécurité
PMP	Plan de management de projet
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
RExpF	Responsable d'exploitation fonctionnelle
RETEX	Retour d'expérience
RF	Responsable fonctionnel
RFE	Responsable fonctionnel d'ensemble
RH	Ressources humaines
RPA	Représentant du pouvoir adjudicateur
RQF	Responsable de quartier fonctionnel
RRP	Responsable de réalisation du projet
RSIC	Responsable es SIC
RSSI - OSSI	Responsable de la sécurité des SI – Officier de sécurité des SI
RTS	Responsable technique de système
RZF	Responsable de zone fonctionnelle
RRZF	Représentant du RZF
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
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



ANNEXE II. COHÉRENCE DES PHASES ET DES JALONS.



ANNEXE III. 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 afin que l'opérateur soit associé à la conduite du projet par la nomination du coordonnateur des activités techniques (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.

- 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-tenu du nouveau système aux tests, cette étape d'intégration est renégociée avec l'opérateur en fonction de la disponibilité de ses équipes.

- L'intégration du SI

- 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 responsable fonctionnel (RF) du projet, et joué par des acteurs fonctionnels ; (tests généralement effectués sur plateforme de pré-production) ;

- 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 (sauf pour les utilisateurs identifiés pour participer à la VABF) (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 batches et de nombre d'utilisateurs maximum et simultanés ; (tests généralement effectués sur plateforme d'intégration) ;

- 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.

- Le déploiement du SI

L'enrôlement du SI au CALID doit être réalisé en préalable du déploiement.

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.

- Mise en production

Cette phase correspond à la mise à disposition du SI à tout ou partie des utilisateurs dans des conditions normales d'utilisation et d'exploitation.

Elle est initiée par une demande de la direction de projet auprès de l'opérateur qui se prononce au regard des livrables qui doivent lui être fournis.

Certains de ces livrables doivent être finalisés et validés parce qu'ils nécessaires à la bonne exploitation et à la sécurité de fonctionnement du SI et de l'ensemble du réseau support.

D'autres doivent être à minima « initialisés », ils seront enrichis au cours de la phase de VSR par un travail collaboratif direction de projet-DIRISI.

Les livrables relatifs à la mise en production :

LIVRABLE :	MATURITÉ.	ACTEURS.
Décision d'homologation, ou <i>a minima</i> , Autorisation provisoire d'exploitation (APE)	APE obligatoire	RSSI-P
Procédure d'exploitation de la sécurité (PES)	Obligatoire	RSSI-P (1), CAT
Procès-verbal de recette fonctionnelle (VA)	Obligatoire	RCP, RF
Procès-verbal de recette technique (VA)	Obligatoire	CAT
Documentation d'architecture (architecture d'échange de flux et matrice de trafic associée ; QoS)	Obligatoire	RCP
Documentation d'installation	Obligatoire	RCP
Documentation d'exploitation	Obligatoire	RCP

Documentation de soutien	Initialisé	RCP, CAT
Fiches réflexes pour les centres d'appels (SDK)	Initialisé	RCP
A minima coordonnées du POC DP ou centre d'expertise.		
Contrat de service (version projet)	Initialisé	RCP, CAT
Contrat d'opération	Obligatoire	RCP

- Le contrat de service

A l'issue des étapes de mise en production et de déploiement, et avec le retour d'expérience de la vérification de service régulier (VSR) (2), 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 politique d'exploitation et de sécurité (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.

(1) Puis lors de la mise en production le RSSI-A rédige si nécessaire la PES définitive ou PES aval.

(2) Remarque : il est important que dès le début de VSR, un projet de contrat de service soit rédigé (direction de projet - exploitant) comportant a minima la procédure de sauvegardes et restauration des données du système. En effet dès le début de VSR le SI traite de données opérationnelles et l'opérateur doit s'engager sur ce point.

ANNEXE IV.
ADMINISTRATION DE DONNÉES.

- 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.

- Mise en œuvre de la démarche d'ADD au ministère

La directive n°14/DEF/DGSIC du 19 juillet 2010 portant sur l'ADD, 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...) 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 :

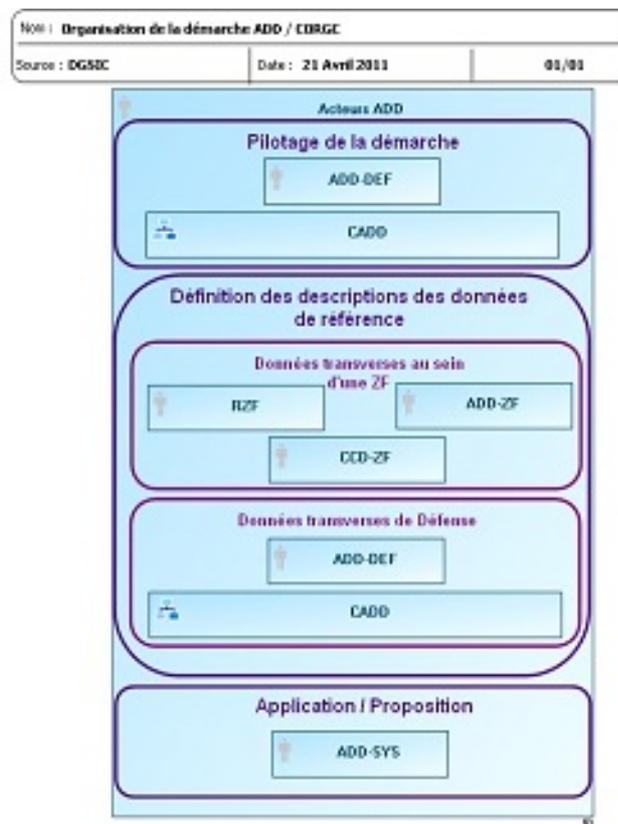
- l'ADD-DEF (administrateur des données Défense) : il pilote la démarche en concertation avec le CADD (voir ci-dessous) et est responsable du processus de définition des données lorsque celles-ci sont utilisées au sein de plusieurs ZF.

- 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).

- l'ADD-SYS (administrateur de données du système) : 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 (comité des administrateurs de données) 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.



- L'ADD au sein d'un projet

Le RF du projet doit nommer, dès le démarrage du projet, l'administrateur de données du système (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 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 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 ;
- 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.

Tout au long de la vie du SI, les avancées de l'ADD doivent figurer dans la fiche SICL@DE conformément au guide de rédaction de cette fiche.

- Contact

Pour toute information relative à la démarche d'ADD, le contact est l'ADD-DEF, à la sous-direction de l'architecture et de l'urbanisation (SDAU) de la DGSIC.

(1) Donnée transverse : donnée échangée ou partagée

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

La loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés stipule que « l'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle 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 » " de données à caractère personnel ou indirectement personnel 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 œuvre , même à titre expérimental, sans qu'il ait été soumis, au préalable, à la Commission nationale de l'informatique et des libertés (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 à caractère personnel, au sens de la loi du 6 janvier 1978 les informations 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 à caractère personnel qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci ;
- 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 dérogations permettent de respecter la confidentialité de certains traitements. Ces traitements sont prévus par le décret n° 2007-914 du 15 mai 2007 pris pour l'application du I de l'article 30 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

2. Les acteurs CNIL.

2.1. Le correspondant général du ministère de la défense.

Afin de faciliter les relations avec la CNIL, la cellule CADA-CNIL-Défenseur des droits de la direction des affaires juridiques (DAJ) est le correspondant unique du ministère de la défense pour l'ensemble des problématiques liées à l'application de la loi du 6 janvier 1978.

Tous les dossiers de déclaration des traitements automatisés de données à caractère personnel préparés par les états-majors, directions et services du ministère de la défense, en particulier par leurs correspondants « informatique et libertés », doivent être transmis à la DAJ aux fins d'expertise.

Ils ne doivent en aucun cas faire l'objet d'une transmission directe ou par télé-procédure à la CNIL ou au commissaire du Gouvernement, sans avoir recueilli l'accord préalable de la DAJ.

Pour les établissements publics placés sous la tutelle du ministre de la défense, seuls les projets de décret en Conseil d'Etat font l'objet d'une transmission à la DAJ, les autres formalités déterminées par la loi du 6 janvier

1978 leur incombent. La DAJ peut néanmoins leur fournir les conseils qu'ils jugent utile de lui demander.

2.2. Les correspondants particuliers des organismes.

Chaque organisme du ministère de la défense doit disposer d'un correspondant particulier, assisté par un suppléant, désigné par l'autorité dont il relève.

Il est par ailleurs conseillé aux établissements publics placés sous la tutelle du ministère de la défense de désigner un interlocuteur unique en charge de ces problématiques, d'en informer la DAJ et de traiter directement avec la CNIL pour les traitements relevant des articles 23, 24 et 25 de la loi du 6 janvier 1978.

Les organismes du ministère de la défense peuvent en outre mettre en place, au sein des différents services placés sous leur autorité, des correspondants afin de faire remonter au niveau central l'ensemble des dossiers relatifs à l'application de la loi du 6 janvier 1978.

Le correspondant particulier centralise alors toutes les demandes transmises par les correspondants subordonnés et assure la coordination de ce réseau interne. Les coordonnées du correspondant particulier sont communiquées à la DAJ, dont il est l'unique interlocuteur sur les questions « informatique et libertés » qui concernent l'organisme qu'il représente.

Par ailleurs, le correspondant adresse chaque année le bilan des demandes de droits d'accès et de rectification que doivent effectuer les directions et services dans le cadre de leur obligation de mise à jour et de rectification des données à caractère personnel traitées.

3. Les procédures.

Les organismes ministériels doivent fonder juridiquement l'existence des traitements de données à caractère personnel dont ils ont la responsabilité. Plusieurs régimes coexistent au regard du contenu des données traitées.

3.1. Régime de la déclaration.

La déclaration est le régime de droit commun pour la plupart des traitements, que ceux-ci relèvent de personnes publiques ou de personnes privées (article 22 de la loi « informatique et libertés »). Elle est un préalable à la mise en œuvre du traitement.

3.1.1. Les fichiers soumis à déclaration.

Il existe deux types de déclarations auprès de la CNIL :

1. La déclaration normale : cette déclaration doit comporter l'engagement que le traitement satisfait aux exigences de la loi (article 23 de la loi « informatique et libertés »). Elle est adressée par la DAJ à la CNIL, qui délivre un récépissé. Le demandeur peut, dès réception de celui-ci, mettre en œuvre le traitement ;

2. La déclaration de conformité à une norme simplifiée : elle concerne les catégories les plus courantes de traitements de données à caractère personnel, dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés (cf. annexe 3). La CNIL établit et publie des normes destinées à simplifier l'obligation de déclaration (article 24 de la loi « informatique et libertés »).

Le cas particulier des « modèles type » défense :

Pour des catégories de traitements couramment mis en œuvre au ministère de la défense mais ne correspondant pas à des normes simplifiées, des « modèles type » défense, validés par la CNIL, ont été publiés au *Bulletin officiel des armées*.

Il existe trois « modèles type » défense relatifs :

- à la gestion des personnels militaires ;
- au contrôle et à la gestion des accès ;
- au suivi du temps de travail.

La déclaration d'un traitement automatisé de données à caractère personnel faite en référence à un « modèle type » défense ne peut concerner qu'un seul service mettant en œuvre le traitement.

Les déclarations de traitements effectuées en référence à ces modèles types suivent la même procédure que celle énoncée pour les normes simplifiées. Toutefois, le formulaire de déclaration simplifiée doit être complété par un engagement de conformité au modèle type défense de référence (cf. annexe 18).

Ce régime déclaratif vaut pour l'ensemble des traitements, à l'exception de ceux soumis à autorisation et entrant dans le champ d'application des articles 25, 26 et 27 de la loi du 6 janvier 1978.

3.1.2. Les fichiers exonérés de déclaration.

Certains fichiers sont exonérés de déclaration :

1. par la loi : elle concerne les traitements pour des activités personnelles (carnets d'adresse, agendas, etc.), les fichiers de membres de partis politiques, d'églises, de syndicats... ;
2. par la CNIL : elle concerne les fichiers de paie, de fournisseurs, de dématérialisation des marchés publics, de blogs, d'associations, de gestion des listes d'adresses, etc.

3.2. Régime de l'autorisation.

3.2.1. Les fichiers soumis à une autorisation de la CNIL.

> Catégorie de traitements concernés :

Les huit catégories de traitements concernées sont énumérées à l'article 25 de la loi « informatique et libertés ». Il s'agit :

- des traitements, automatisés ou non, mentionnés au 7° du II, au III et au IV de l'article 8 de la loi^[1] ;
- de certains traitements automatisés portant sur des données génétiques ;
- de certains traitements automatisés ou non, portant sur des données relatives aux infractions, condamnations ou mesures de sûreté ;
- des traitements automatisés ayant pour objet l'interconnexion de fichiers relevant d'une ou de plusieurs personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents ou relevant d'autres personnes et dont les finalités principales sont différentes ;
- des traitements portant sur des données parmi lesquelles figure le NIR et ceux qui requièrent une consultation de ce répertoire sans inclure ce numéro d'inscription ;
- de ceux qui comportent des appréciations sur les difficultés sociales des personnes ;
- de ceux qui comportent des données biométriques nécessaires au contrôle de l'identité des personnes.

Autorisation par décision unique :

En outre, peuvent être autorisés par une décision unique de la CNIL, les traitements qui :

- répondent à une même finalité ;
- portent sur des catégories de données identiques ;
- ont les mêmes destinataires ou catégories de destinataires.

3.2.2. Les fichiers soumis à autorisation par acte réglementaire.

Les articles 26 et 27 de la loi du 6 janvier 1978 prévoient les cas dans lesquels les traitements doivent être autorisés par un acte réglementaire, pris après avis motivé et publié de la CNIL.

L'article 26 dispose que les traitements de données à caractère personnel qui nécessitent une autorisation par arrêté ministériel sont ceux, mis en œuvre pour le compte de l'État, qui intéressent la sûreté de l'État, la défense nationale ou la sécurité publique ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté lorsqu'ils ne contiennent pas de données sensibles.

Selon l'article 26-II et l'article 27 de la loi de 1978, lorsque les traitements portent sur des données dites « sensibles », ils sont soumis à une autorisation formalisée par décret en Conseil d'État, pris après avis motivé et publié de la CNIL.

Sont autorisés par décret en Conseil d'État :

- les traitements mis en œuvre par l'État et intéressant la sûreté, la défense nationale ou la sécurité publique contenant des données sensibles ;
- les traitements comportant des données biométriques ;
- les téléservices de l'administration électronique ;
- les traitements du recensement ;
- les traitements du secteur public comportant le numéro d'inscription au répertoire national d'identification des personnes physiques (NIR).

Pour ces traitements, l'article 27 opère une distinction entre les traitements dans lesquels le NIR est enregistré et ceux qui requièrent une simple consultation. Seuls les traitements dans lesquels le NIR est enregistré font l'objet d'un décret en Conseil d'État (article 27-I-1°)

Sont autorisés par arrêté ou par décision de l'organe délibérant des établissements publics :

- les traitements qui requièrent une simple consultation du répertoire national d'identification des personnes physiques sans inclure le numéro (article 27-II-1°) ;
- toutefois, si ce traitement comporte des données à caractère médical, il est soumis à un décret en Conseil d'État.

3.2.3. Comment procéder à une demande d'autorisation ?

La procédure classique, l'accord du Commissaire du Gouvernement :

Pour l'ensemble des traitements entrant dans le champ d'application des articles 25, 26 et 27 de la loi de 1978, le correspondant ministériel sollicite le commissaire du Gouvernement auprès de la CNIL, afin de recueillir son avis préalablement au dépôt du dossier à la CNIL.

La CNIL a alors deux mois à compter de la réception de la demande pour rendre un avis. Ce délai peut être renouvelé une fois sur décision motivée de son président.

Le dossier est alors étudié en assemblée plénière et la CNIL prend une délibération. Cette délibération vaut avis ou autorisation.

Pour les traitements entrant dans le champ d'application de l'article 25 de la loi de 1978, si la CNIL ne se prononce pas dans les délais, la demande d'autorisation est réputée rejetée. Pour ceux entrant dans le champ d'application des articles 26 et 27, si la CNIL ne se prononce pas dans ce délai, l'avis est réputé favorable.

4. Comment faire valider un projet de déclaration CNIL ?.

4.1. L'accord obligatoire de la direction des affaires juridiques.

Aucun organisme du ministère de la défense n'est autorisé à correspondre directement avec la CNIL ou avec le commissaire du Gouvernement.

Les dossiers de déclaration qui sont adressés directement à la CNIL sans être passés par la DAJ ne sont pas instruits par la commission et sont renvoyés au correspondant ministériel.

Une fois remplis, les formulaires, leurs annexes et les projets de textes correspondants (décret ou arrêté) sont transmis pour instruction et centralisation au correspondant particulier de l'état-major, de la direction ou du service dont relève le déclarant.

Ce correspondant procède aux corrections nécessaires et soumet ensuite son projet, par voie électronique, à l'analyse et à la validation de la cellule CADA-CNIL-Défenseur des droits de la DAJ.

Une fois validés par le correspondant ministériel, les formulaires sont signés par l'autorité délégataire de la signature du ministre en matière « informatique et libertés », conformément au décret du 27 juillet 2005. Le dossier est alors transmis, par bordereau d'envoi, à la DAJ pour dépôt du dossier à la CNIL.

4.2. Suivi de la procédure de déclaration normale.

Après le dépôt du dossier à la CNIL par la DAJ, le correspondant ministériel adresse, au service émetteur, un reçu de dépôt du dossier. La CNIL instruit le dossier. Elle envoie ensuite un récépissé de déclaration à la DAJ et au correspondant CNIL de l'état-major, direction ou service responsable du traitement, afin que le service puisse mettre en œuvre le traitement.

Aux fins d'opposabilité aux tiers, et afin de garantir le droit à l'information des personnes concernées par le traitement de données à caractère personnel, un arrêté ministériel portant création du traitement est élaboré par le service chargé de la mise en œuvre du traitement en liaison avec la DAJ, puis publié après validation de la DAJ, par le déclarant, au *Bulletin officiel des armées*.