BULLETIN OFFICIEL DES ARMÉES

Édition Chronologique n° 93 du 11 juin 2019

TEXTE RÉGLEMENTAIRE PERMANENT

Texte 2

INSTRUCTION N° 2476/ARM/CAB/CC6

portant sur la conduite des projets de système d'information et de communication.

Du *29 avril 2019*

CABINET DE LA MINISTRE :

INSTRUCTION N° 2476/ARM/CAB/CC6 portant sur la conduite des projets de système d'information et de communication.

Du 29 avril 2019

NOR A R M M 1 9 5 4 0 7 7 J

Référence(s) :
Voir annexe III

Pièce(s) jointe(s) :
Trois annexes

Texte(s) abrogé(s) :
- Instruction MINISTÉRIELLE N° 2007/DEF/DGSIC du 24 mars 2014 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.
- Instruction N° 2008/DEF/DGSIC du 10 juillet 2013 fixant les modalités d'approbation et de suivi des systèmes d'information et de communication.

Classement dans l'édition méthodique :
BOEM 160.3.

Référence de publication :

Préambule.

L'instruction relative aux opérations d'investissement (OI) du ministère des armées (*Cf.* annexe III, référence 9) définit les objectifs et principes applicables à ces investissements, leur gouvernance et les modalités de conduite et de suivi des projets.

Les opérations d'investissement relatives aux systèmes d'information et de communication (SIC) portent la performance numérique du ministère et une part croissante de sa performance opérationnelle.

Ces opérations d'investissement SIC se distinguent par :

- un besoin fonctionnel évolutif, qui se stabilise en cours de développement dans le cadre d'un dialogue constant entre utilisateurs et développeurs. Cette caractéristique nécessite une conduite en cycles courts et en prise directe avec les utilisateurs ;

- un contexte de transformation des métiers. Pour beaucoup d'entre eux, ces projets SIC accompagnent des démarches de numérisation et de modernisation des processus. Il s'agit également de transformer progressivement les organisations et les modes de fonctionnement ;

- une part prépondérante des développements logiciels, qui permet d'adopter les meilleures pratiques de développement incrémental émergeant du secteur civil ;

- l'importance de la prise en compte des données, dont la qualité et l'exploitation conditionnent la performance globale du système ;

- l'intégration nécessaire, dès leur conception, des principes de protection en matière de cyberdéfense afin de diminuer la vulnérabilité des systèmes.

Mettant l'accent sur les données et les services aux utilisateurs l'organisation en plateforme[1] s'accommode mal du cycle classique « en V »[1] de développement d'un nouveau système en remplacement d'un ancien. En revanche les approches agiles de gestion de projet[2], utilisant des expérimentations (POC)[1] pour affiner les nouveaux processus, et des « produits minimum viables » (PMV)[1] comme première briques testables à l'échelle du projet, permettent de développer, par incréments fonctionnels, le système d'information cible.

C'est d'autant plus vrai que les technologies de l'informatique en nuage (« *cloud computing* ») transforment aujourd'hui les modèles de développement et d'exploitation des systèmes d'information, en permettant :

- des modes de développement et de mise en service rapide d'incréments fonctionnels ;

- la constitution de zones de partage des données (dits « puits de données »)[1] à un juste niveau de cybersécurité, permettant un recours facilité aux outils de « *Big data* » et d'intelligence artificielle (IA).

1. OBJET DE L'INSTRUCTION.

La présente instruction a pour objet de préciser les modalités de conduite des opérations d'investissement SIC non érigées en opération d'armement (projets SIC), en particulier le contenu des travaux à réaliser au cours de différentes phases tout en précisant les responsabilités des acteurs du projet. Pour les projets SIC les plus complexes ou portant des enjeux spécifiques, des dispositions complémentaires en matière de gouvernance peuvent être appliquées.

En outre une opération d'investissement, conduite dans le cadre des opérations d'armement relevant de l'instruction n°1618/ARM/CAB du 15 février 2019 (*Cf.* annexe III, référence 10), pourra utilement s'inspirer des principes méthodologiques décrits dans la présente instruction dès lors que celle-ci inclue une composante SIC.

2. PRINCIPES GÉNÉRAUX.

2.1. **Domaine d'application.**

La conduite des projets SIC, qui concourent aux opérations, au fonctionnement et à la transformation numérique du ministère, est placée sous la responsabilité du chef d'état-major des armées (CEMA), du secrétaire général pour l'administration ou du délégué général pour l'armement selon le « segment » considéré, c'est-à-dire respectivement les systèmes d'information opérationnels et de communication (SIOC), les systèmes d'administration et de gestion (SIAG) ou les systèmes d'information scientifiques et techniques (SIST).

Ces projets répondent aux besoins exprimés par les armées, directions et services (ADS). Dans la suite du document, l'organisme porteur du besoin est appelée autorité cliente (AC)[3]. Ces projets sont validés par l'état-major des armées (EMA), la direction générale de l'armement (DGA) et le secrétariat général pour l'administration (SGA), dans leur segment respectif de responsabilité. Pour les projets relevant du socle numérique du ministère, le besoin est porté par la direction générale du numérique et des systèmes d'information et de communication (DGNUM)[4].

La présente instruction définit les modalités de conduite, de vérification, de contrôle et d'approbation des projets SIC. Elle s'applique à l'ensemble des SIOC, SIAG ou SIST, hors opération d'armement. Elle définit les conditions de suivi en service des produits livrés tout au long de leur cycle de vie. Elle contribue à la rationalisation du parc applicatif et à la convergence des besoins.

Pour les services et produits numériques régis par l'instruction relative à la conduite agile des services digitaux (*Cf.* annexe III, référence 7), cette instruction s'applique à compter de l'élaboration du dossier de réalisation, dès lors qu'une décision de passage à l'échelle a été prise.

Conformément aux dispositions de l'instruction n°100/ARM/CAB du 15 février 2019 relative aux opérations d'investissement, chaque projet SIC fait l'objet d'un dossier entretenu tout au long du cycle de vie, permettant de documenter l'ensemble des informations pertinentes pour son suivi, d'instruire les changements de phase, d'assurer la traçabilité des décisions prises et de mesurer l'atteinte des objectifs fixés à travers des indicateurs de performance. Cette documentation est traitée de manière dématérialisée dans l'application SICL@DE, opérée par la DGNUM.

Enfin, les projets SIC qui relèvent du périmètre du système d'information de l'État[5], veillent à prendre en compte les principes de mutualisation[6] adoptés en interministériel et diffusés par la direction interministérielle du numérique et du système d'information et de communication (DINSIC).

2.2. **Phasage général des projets de systèmes d'information et de communication.**

2.2.1. ***Les différentes phases.***

Le processus général de conduite des projets SIC comporte trois phases principales :

1. la phase de préparation, qui comprend l'orientation, la spécification générale et détaillée, ainsi que la définition du calendrier général du projet, du devis estimé et de la stratégie d'acquisition ou de développement[7], et se termine par une revue de changement de phase ;

2. la phase de réalisation**,** qui comprend la phase de consultation, la notification des marchés nécessaires, le développement, et se termine par la mise en service opérationnel (MSO). Au sein de la phase de réalisation, on distingue une phase de primo-réalisation d'un cœur initial de fonctionnalités (ou PMV[8]), permettant de cerner et de concrétiser rapidement les besoins prioritaires des utilisateurs, de les expérimenter et de les consolider. S'en suit une phase combinée d'utilisation généralisée de ce PMV et de réalisation des fonctionnalités complémentaires ;

3. La phase d'utilisation qui se termine au terme des opérations de retrait de service.

Ce processus est conduit par une équipe de projet pilotée par un responsable de conduite de projet (RCP) désigné par l'autorité cliente et constituée d'experts désignés dans les domaines fonctionnel, technique et sécurité numérique[9]. Le RCP veille à associer les futurs utilisateurs à toutes les étapes du projet.

2.2.2. ***Les changements de phase.***

Les projets SIC inscrits dans la liste des opérations d'investissement (LOI) relèvent, pour l'approbation de leurs changements de phase, soit du comité ministériel des investissements soit de la commission d'examen des investissements (CEI).

Le contrôle physico financier des autres projets SIC est assuré par l'autorité en charge du segment concerné, qui s'appuie sur les commissions mentionnées au chapitre II de l'arrêté du 28 juin 2018 portant crétation et organisation d'instances relatives au système d'information et de communication de la défense (*Cf.* annexe III, référence 3). Ces commissions, compétentes en matière de SIOC, de SIST ou de SIAG, sont placées respectivement sous l'autorité du CEMA, du DGA et du SGA au titre de leurs attributions. Ils en organisent, à leur niveau, les modalités de fonctionnement et de délégation.

Ces commissions doivent permettre à ces autorités de s'assurer que :

- le portefeuille applicatif est et reste aligné sur la politique des SI du ministère et sur les schémas directeurs des segments ;

- la contribution de tout nouveau projet à la modernisation du ministère et à la rationalisation du SI est correctement évaluée. Il fait pour cela l'objet d'une étude d'impact et d'une approbation formelle du responsable de la zone fonctionnelle afférente (RZF)[10] ;

- tout projet fait l'objet d'une étude de la valeur (rapport coût de réalisation et de déploiement / service rendu)[11] ;

- tout projet présente des garanties de cohérence fonctionnelle ainsi que de cohérence d'architecture, de faisabilité et de soutenabilité ;

- tout projet présente une stratégie de management relative aux données en définissant à la fois son besoin en protection mais aussi en partage. Cette stratégie fait l'objet d'une approbation par le ou les directeurs de données concernés[12] ;

- les conditions de réussite du projet sont réunies : en particulier les acteurs indispensables à la réussite du projet doivent y être impliqués à bon niveau ; et le cadre

de conduite choisi doit être adapté aux enjeux du projet ;

- les systèmes en service sont suivis régulièrement, jusqu'au retrait de service ;

- les ressources (financières et humaines) allouées aux projets ou aux systèmes en service existent, sont pilotées et définis au plus juste besoin.

2.2.3. ***Le pilotage des projets.***

Un projet est piloté par un comité directeur (CODIR) de projet mis en place dès l'approbation du dossier de lancement (*Cf.* point 3.1). Le CODIR est chargé de superviser la conduite du projet, dans toutes ses composantes, et la réalisation de ses objectifs.

Il est composé, au minimum, de l'autorité cliente, qui le préside, des autres ADS utilisatrices, du responsable de conduite du projet et son équipe, d'un représentant du pouvoir adjudicateur le cas échéant, et du ou des responsables de zone fonctionnelle concernés ou leur représentant.

Le responsable de segment dont relève le projet peut décider, en fonction de sa complexité, de la mise en place de comités complémentaires[13].

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 CEMA[14], après avis de la DGA ou de la direction interarmées des réseaux d'infrastructure et des systèmes d'information (DIRISI) selon la nature du besoin. L'EMA informe la DGNUM de cette décision. 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, notamment dans ses aspects financier, technique et capacitaire.

3. PHASE DE PRÉPARATION.

3.1. **Étude préalable.**

Préalablement à la réalisation de tout projet SIC, une phase d'étude permet de formaliser l'expression du besoin initial ou d'une évolution majeure du système[15]. Cette étude est entièrement placée sous la responsabilité de l'autorité cliente du système et requiert le soutien du ou des responsables des zones fonctionnelles concernées ainsi que du ou des directeurs de données concernés.

Une étude de faisabilité est initiée (technique, management du projet et impacts organisationnels…) qui est destinée à fixer le périmètre, à identifier les options possibles (développement spécifique, achats sur étagère, modernisation d'un système existant…).

Cette étude détermine en particulier le ou les modes de conduite les plus adaptés à la finalité recherchée (exemple : une combinaison entre méthode « cycle en V » pour un PMV conséquent et « agile » pour les incréments fonctionnels).

L'étude préalable est close sur décision du responsable de segment concerné au vu du dossier de lancement (DL) élaboré durant cette phase.

3.2. **Spécification.**

La phase de spécification permet d'identifier les grandes fonctions (analyse fonctionnelle), leurs cadres normatif et réglementaire, de caractériser les performances, les besoins d'interopérabilité, les exigences en matière de protection des données personnelles et de sécurité des systèmes d'information (SSI) ainsi que de soutien, la stratégie de consommation et de mise à disposition des données et services en provenance ou au profit des autres systèmes d'information (au travers d'une stratégie d'API[16]), les risques (juridiques[17], techniques, financiers et calendaires), de mener l'analyse de la valeur et de construire la soutenabilité du projet (ressources financières, ressources humaines en MOA, ressources humaines en MOE dans le cas du choix d'un développement interne).

Elle comprend en outre une estimation du calendrier du projet, la prise en compte de la conduite du changement ainsi que, le cas échéant, une estimation du retour sur investissement.

Cette phase peut donner lieu à la réalisation de démonstrateurs ou preuve de concept[16] permettant de lever des incertitudes auprès des futurs utilisateurs du système.

En fonction de la complexité du projet, le responsable de segment concerné peut demander à l'AC la présentation d'un dossier de spécification (DS).

Cela permet d'arrêter, parmi les options, l'orientation retenue, réduire les risques, décrire les grandes fonctions et performances associées, les cas d'usage, le périmètre, les interfaces et l'environnement, le système de soutien, la stratégie d'acquisition, la conduite du changement nécessaire, les moyens et organisations nécessaires, les délais, les feuilles de route, les formations nécessaires. On veillera également à détourer le cœur de fonctionnalités, qui fera l'objet de la phase prioritaire de primo-conception.

Le plan de développement associé identifiera le cas échéant la stratégie de PMV à mettre en œuvre en phase de réalisation, caractérisée par :

- des cycles courts de création / production ;

- un retour constant des besoins utilisateurs ;

- un focus sur l'amélioration des fonctionnalités de base.

3.3. **Clôture de la phase de préparation.**

La phase de préparation doit permettre aux acteurs du projet de justifier :

- le respect du besoin exprimé et le périmètre du projet, sa formalisation sous formes d'exigences suivies, la rédaction d'un cahier des clauses techniques particulières, la mise en œuvre des dispositions du plan de management du projet et leur actualisation ;

- la détermination du coût de référence du projet, de l'affectation des ressources financières et humaines nécessaires et son management (maîtrise du budget du projet, échéancier de facturation, coût global) et des gains attendus (dispositif de suivi du retour sur investissement) ;

- la détermination de la durée de référence du projet, son management (planning, phases clés, charges, maitrise de l'avancement) et son séquencement [calendrier des opérations détaillant les phases retenues pour la conduite du projet, et permettant d'aboutir à la vérification de service régulier (VSR)] ;

- le plan de management du projet, qui doit préciser l'attribution des responsabilités, l'organisation nécessaire mise en place, notamment pour prendre en compte le retour d'expérience des futurs utilisateurs tout au long du projet, le management des risques, 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 soient bien identifiés, un cumul de fonctions par une même personne restant possible ; pour les projets conduits selon une approche Agile (SAFe®, SCRUM, etc.) le plan de management, limité au strict nécessaire, définira les rôles spécifiques de ces méthodes (*Cf.* glossaire) ;

- la mise en place d'une démarche de sécurité des systèmes d'information sur le projet, permettant l'homologation du système mis en production avant la fin de réalisation, comprenant la prise en compte des exigences de cyberdéfense, dont notamment l'enrôlement au CALID ;

- la prise en compte de la protection des données personnelles, si le système doit en traiter[18], dont l'élaboration le cas échéant de l'analyse d'impact et la mise à jour du registre des traitements (sur SICL@DE) dans le cadre du règlement général sur la protection des données (RGPD)[19];

- la contribution à la convergence des systèmes et la maîtrise des interfaces, dans le respect du cadre d'architecture générale et de cohérence technique (normes et standards ministériels…) ;

- la stratégie de mise à disposition des données et services produits par le système (stratégie API) et les modalités de leur gouvernance[18] ;

- la stratégie d'acquisition ;

- la stratégie de vérification d'aptitude ;

- la maîtrise de son intégration au socle technique commun en matière d'hébergement et d'exploitation par la DIRISI, ou l'hébergeur pressenti ;

- les modalités du déploiement et de conduite du changement ;

- l'organisation et les choix retenus pour le maintien en condition opérationnelle et le maintien en condition de sécurité (MCO/MCS) ;

- la stratégie d'archivage des contenus du système d'information ;

- la mise à jour de l'outil de gestion du portefeuille SIC (SICL@DE).

En fonction des caractéristiques du projet (coût de référence, fort enjeu ministériel, appartenance au système d'information de l'État[20]), un visa conforme de la DINSIC[21], ou de la DGNUM[22] peut être nécessaire pour autoriser le changement de phase.

L'ensemble des documents produits constitue le dossier de réalisation (DR), y compris pour les services et produits numériques régis par l'instruction relative à la conduite agile des services digitaux (*Cf.* annexe III, référence 7) pour lesquels une décision de passage à l'échelle a été prise.

La phase de préparation se termine par une revue du DR, organisée par le responsable du segment correspondant, ou pour les projets inscrits dans la liste des opérations d'investissement (LOI), par le secrétariat permanent aux investissements (CEI ou CMI).

4. PHASES DE RÉALISATION ET D'UTILISATION.

Le franchissement de la phase de préparation permet la publication d'une consultation pour la réalisation du système. En fonction de la procédure retenue, la publication d'un avis de mise en concurrence permettant la sélection des candidatures peut être anticipée en phase de spécification détaillée, dès lors que la remise du dossier de consultation des entreprises (DCE) est prévue après le franchissement de la phase de préparation.

Les phases de réalisation et d'utilisation ont pour objectif de mettre en œuvre la démarche d'acquisition ou de réalisation interne définie (notification des marchés ou contrats de service nécessaires), de réaliser le projet, de l'homologuer, de le mettre en service opérationnel et d'en assurer la maintenance et l'amélioration continue, grâce :

- au maintien en condition opérationnel (MCO) et de sécurité (MCS) des composants déployés ;

- à l'enrichissement des fonctionnalités initiales du projet par un processus continu d'amélioration et de gestion des évolutions du système.

4.1. **Les conditions de réussite du projet.**

En fonction de la sensibilité et de l'importance du projet, des dispositions sont prises par le RCP pour s'assurer du respect du besoin exprimé et validé, et en mettant en œuvre un processus de retour d'expérience des futurs utilisateurs.

Un suivi périodique des risques, des délais, des coûts et des gains attendus est assuré par le RCP, en particulier pour les projets relevant d'un avis conforme DINSIC ou DGNUM.

4.2. **Cohérence technique du projet.**

Une attention particulière est portée par le RCP, pendant toute la phase de réalisation et d'amélioration continue, sur la maitrise technique des interfaces avec les autres systèmes d'information, en particulier dans le cadre de l'utilisation ou de la production de données ou de services au travers de la mise en œuvre de la

stratégie d'API définie.

Les modalités techniques d'hébergement et de déploiement sur l'internet ou le socle informatique du ministère, et, le cas échéant, de son exploitation par la DIRISI sont établies.

4.3. **Préparation de la mise en service.**

Elle doit s'attacher à définir et mettre en œuvre les modalités de formation, d'accompagnement au changement, de mise en service et de soutien tant matériel que logiciel.

Elle couvre également le suivi de la qualification du système, préparatoire à la vérification d'aptitude (VA) et à l'homologation. À cet effet :

- un plan d'essais, découlant de la stratégie de VA, est défini (organisation des essais, scénarios de test, cas de test). Son ampleur est fonction de l'importance du projet ;

- la démarche de tests et d'audits est soumise à l'autorité d'homologation.

Cette phase de réalisation se termine à l'issue de la vérification de service régulier (VSR), de la mise en place du MCO initial et de l'homologation du système.

L'ensemble des documents produits constitue le dossier d'utilisation (DU).

La phase de réalisation se termine par une revue du DU, organisée par le responsable du segment correspondant, ou pour les projets inscrits dans la liste des opérations d'investissement (LOI), par le secrétariat permanent aux investissements (CEI ou CMI).

La mise en service opérationnelle du SI fait l'objet d'une décision de l'autorité cliente, dès lors que le changement de phase est approuvé.

4.4. **Soutien en service.**

Le responsable technique du système (RTS) remplace le responsable de conduite de projet en phase d'utilisation. Il est désigné par l'autorité cliente en amont de la mise en service opérationnelle et s'appuie sur les compétences techniques de l'opérateur qui exploitera le système. Il est responsable de la phase d'utilisation du système qui recouvre :

- l'exploitation du système ;

- la maintenance et l'amélioration continue du système (MCO) ;

- le maintien en condition de sécurité du système (MCS) ;

- le soutien aux utilisateurs ;

- la gestion des évolutions du système (avec le traitement des éventuels impacts liés à l'homologation, aux données, y compris personnelles, aux interfaces, au MCO/MCS, etc. mis en place initialement).

La fonction « MCO/MCS » 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 et de la sécurité du système en exploitation, par des actions de maintenance ;

- le traitement des incidents ;

- le traitement des obsolescences.

La fonction « exploitation » assure l'exploitation et la supervision quotidiennes du système, ainsi que la gestion des incidents, matériels ou logiciels, relatifs au fonctionnement du SI. Cette fonction doit également s'assurer que le SI est correctement soutenu dans son environnement de déploiement et prend en compte ses contraintes (échanges avec des fonctions externes de type NOC/SOC et/ou hébergement).

La fonction « 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, ainsi que des exigences dans le cadre de la mise en œuvre du RGPD.

La fonction « gestion des évolutions » assure l'instruction et le pilotage des demandes d'évolution (y compris les évolutions majeures, nécessitant un retour en mode projet).

4.5. **Retrait de service.**

Le retrait de service d'un système d'information s'inscrit dans une démarche de maitrise du patrimoine applicatif et doit être anticipé. À cette fin, les responsables de segment identifient, via les responsables SIC des organismes et les informations contenues dans SICL@DE, les systèmes dont la fin de vie prévisionnelle est inférieure à deux ans, afin d'en anticiper tous les impacts.

Après consultation des ADS utilisatrices de ces systèmes, l'autorité cliente établit, avec le service historique de la défense (SHD), le dossier de retrait de service (DRS) et le soumet à la validation du responsable de la zone fonctionnelle concernée. La commission *ad hoc* statue alors sur le décommissionnement des applications, qui sera effectué par l'hébergeur de l'application.

Le sort réservé aux données générées par le SI est défini dans la stratégie d'archivage élaborée avec le soutien du SHD (dès la phase de préparation du projet[23]) et entretenue durant toute la vie du système.

5. DISPOSITIONS PARTICULIÈRES.

Les dispositions applicables aux projets SIC conduits en interministériel font l'objet de dispositions particulières prises au cas par cas.

6. TEXTES ABROGÉS.

Les instructions suivantes sont abrogées :

- instruction n° 2008/DEF/DGSIC du 10 juillet 2013 fixant les modalités d'approbation et de suivi des systèmes d'information et de communication ;

- instruction n° 2007/DEF/DGSIC du 24 mars 2014 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.

7. PUBLICATION.

La présente instruction est publiée au *Bulletin officiel des armées*.

Notes

[1] *Cf.* annexe II.

[2] *Cf.* annexe III, référence 13.

[3] Dans le cas de projets répondant à des besoins transverses, l'AC veille à agréger les besoins des autres ADS, en particulier les conditions de mise en œuvre du projet et les objectifs de sécurité de leur responsabilité (modes de travail, processus, articulation avec d'autres métiers, ...).

[4] Les autres organismes dépendant directement du ministre s'intègrent dans ce dispositif pour leurs SI ou peuvent faire l'objet de dispositions particulières.

[5] Les projets de SIAG.

[6] https://www.numerique.gouv.fr/publications/principes-mutualisation-si-etat/

[7] Intégration au plan de charge d'un centre de développement interne par contrat de service.

[8] *Cf.* annexe II.

[9] *Cf.* instruction PSSI-M citée en annexe III, référence 5.

[10] *Cf.* à ce sujet le guide cité en annexe III, référence 12.

[11] Pour les projets SIC à fort enjeu ministériel, la méthode d'analyse de la valeur utilisée au sein du ministère est la méthode MAREVA 2 (*Cf.* annexe II).

[12] *Cf.* instruction citée en annexe III, référence 8.

[13] Comité de pilotage au niveau du RCP, comité d'orientation fonctionnelle dans le cas d'un projet d'ensemble, comité de gestion de configuration, comité utilisateur ...

[14] Dans l'esprit de l'instruction n° 52607/DEF/DGA/DO - n° 103/DEF/EMA/PLANS du 25 mars 2014 relative à la procédure d'urgence opérationnelle.

[15] En particulier, sont considérées comme des évolutions majeures :

- une refonte technologique ou une évolution significative d'architecture ;

- un changement de la confidentialité, intégrité, disponibilité des données ou des fonctions du SI ;

- l'ajout, la modification ou la suppression de fonctions ou d'équipements de sécurité ;

- une modification à la baisse de l'agrément ou de la qualification d'un équipement de sécurité ;

- la modification de la stratégie d'homologation ;

- une évolution des interconnexions ou une extension à des utilisateurs hors ministère.

[16] *Cf.* annexe III, références 8 et 14 et annexe II.

[17] Tout particulièrement au regard des données qui seront traitées par le système.

[18] Le partage de données étant le principe, conformément à l'instruction citée en annexe III, référence 8, relative à la gouvernance ministérielle des données, la non mise à disposition ou une mise à disposition limitée ou restreinte des données doit être justifiée (ex : protection du secret des secrets légaux, confidentialité de la donnée, etc.).

[19] *Cf.* à ce sujet l'instruction citée en annexe III, référence 6, relative à la mise en œuvre du règlement européen pour la protection des données personnelles au ministère de la défense.

[20] Seuls les SIAG font partie du système d'information de l'État.

[21] *Cf.* arrêté cité en annexe III, référence 2.

[22] *Cf.* arrêté cité en annexe III, référence 4.

[23] Directive citée en annexe III, référence 11 (https://synoptic.intradef.gouv.fr/ressource-documentaire/directive-ndeg30defdgsic-du-05-decembre-2013-portant-sur-la-mise-en-oeuvre-de).

ANNEXE I.
SCHÉMA TYPIQUE DU DÉROULEMENT D'UN PROJET DE SYSTÈME D'INFORMATION ET DE COMMUNICATION.

/render/cke/resource/1a1fd26e-86cd-11e9-b0cf-005056a225e8.pdf

ANNEXE II.
GLOSSAIRE.

/render/cke/resource/284eb300-86cd-11e9-9cdd-005056a225e8.pdf

ANNEXE III.
TEXTES DE RÉFÉRENCE.

Textes de références.

1. Décret n° 2018-532 du 28 juin 2018 fixant l'organisation du système d'information et de communication de la défense et portant création de la direction générale du numérique et des systèmes d'information et de communication (JO du 29 juin 2018, texte n° 13) ;

2. Arrêté du 14 novembre 2014 pris pour l'application de l'article 3 du décret n° 2014-879 du 1er août 2014 relatif au système d'information et de communication de l'État (JO du 16 novembre 2014, texte n° 5) ;

3. Arrêté du 28 juin 2018 portant création et organisation d'instances relatives au système d'information et de communication de la défense ;

4. Arrêté du 28 juin 2018 pris pour l'application de l'article 5 du décret n° 2018-532 du 28 juin 2018 fixant l'organisation du système d'information et de communication de la défense et portant création de la DGNUM (JO du 29 juin 2018, texte n° 16) ;

5. Instruction n° 7326/ARM/CAB du 25 juin 2018 relative à la politique de sécurité des systèmes d'information du ministère des armées (PSSI-M) ;

6. Instruction ARM/SGA/DAJ/D2P du 19 juillet 2018 relative à la mise en œuvre du règlement européen pour la protection des données personnelles au ministère de la défense ;

7. Instruction n° 1/ARM/DGNUM/NP du 5 octobre 2018 relative à la conduite agile des services digitaux (n.i. BO) ;

8. Instruction n° 2/ARM/DGNUM/NP portant sur la gouvernance ministérielle des données (édition approuvée le 15 octobre 2018 - n.i. BO) ;

9. Instruction n° 100/ARM/CAB du 15 février 2019 relative aux opérations d'investissement du ministère des armées ;

10. Instruction n° 1618/ARM/CAB du 15 février 2019 sur le déroulement des opérations d'armement ;

11. Directive n° 30/DEF/DGSIC du 5 décembre 2013 portant sur la mise en œuvre de la démarche d'archivage des contenus dans les projets de systèmes d'information du ministère de la défense ;

12. Guide du responsable de zone fonctionnelle (1re édition, approuvée le 17 avril 2014 - n.i.BO) ;

13. Guide DGSIC n° 15/ARM/DGSIC/NP portant sur l'agilité dans le cadre de la transformation numérique (1re édition, approuvée le 4 mai 2018 - n.i. BO) ;

14. Cadre technique de mise en œuvre des API au sein du ministère des armées (V 1.0 du 21 février 2019 - n.i. BO).

La ministre des armées,

Florence PARLY.