

Paris, le 25 février 2026
N° DEP-00106/2026/ARM/DPID/NP

NOTE

OBJET : mise à jour de la directive ministérielle portant sur l'homologation des systèmes d'information du ministère des armées

REFERENCE : note n°DEP-00337/2022/ARM/DPID/NP du 7 juin 2022 relative à la troisième édition de la directive n°27 portant sur l'homologation des systèmes d'information du ministère.

ANNEXE : Version 3.1 de la directive 27.

Les missions du ministère des Armées reposent sur des systèmes d'information (SI) toujours plus nombreux, souvent interconnectés entre eux, voire avec notre environnement interministériel ou avec l'industrie. Ces systèmes évoluent également à très grande vitesse, que ce soit avec l'IA aujourd'hui ou l'avènement de l'informatique quantique demain. Cette dynamique va entraîner l'apparition de nouvelles failles ou vulnérabilités, d'autant plus problématiques en matière de cybersécurité que nos infrastructures informatiques - comme celles des établissements publics sous tutelle et de nos fournisseurs - feront inévitablement l'objet d'un ciblage spécifique de la part d'attaquants ou de compétiteurs stratégiques qui tous testeront notre résilience et les moyens d'entraver nos activités. Toutes ces raisons nous incitent à porter une attention accrue à la sécurisation des systèmes d'information, à leur bon fonctionnement et donc à leur maîtrise.

La cartographie des SI et leur homologation sont un préalable à toute démarche de sécurisation. La démarche d'homologation, notamment, permet de connaître le périmètre et l'état de sécurité d'un système d'information, d'évaluer les risques qui pèsent sur les capacités opérationnelles auxquelles ce SI contribue, et d'assurer ainsi dans la durée la prise en compte au juste niveau des besoins de sécurité.

Pourtant, bien que la finalité de l'homologation ne soit pas remise en cause, sa mise en œuvre demeure longue et complexe. Les délais et coûts induits par le processus d'homologation génèrent un effet d'éviction et donc des zones de fragilité dans le développement et le soutien des systèmes d'information. En outre, mal comprise, l'homologation pourrait devenir à terme un exercice de conformité administrative alors qu'elle constitue le premier rempart de notre système de protection par la maîtrise des risques.

La présente révision de la Directive 27 vise à donner des premiers outils de simplification du processus d'homologation. Elle doit permettre aux AQSSI d'homologuer plus de systèmes avec les mêmes ressources, et ce sans dégrader le niveau de sécurité grâce à des méthodes pragmatiques et à une dématérialisation des processus. Elle s'appuie sur les orientations de l'Agence nationale de sécurité des systèmes d'information (ANSSI) et sur un travail collégial avec les centres experts du domaine de l'homologation et les représentants des autorités qualifiées du ministère.

Il est demandé à l'ensemble des AQSSI et entités impliquées dans les processus d'homologation de mettre en œuvre dès à présent les modalités techniques issues de la présente directive.

Un retour d'expérience de la mise en œuvre de cette révision de la Directive 27 sera réalisé dans 6 mois.

Le général de division aérienne Nicolas Leverrier,

Directeur de la protection des installations,
moyens et activités de la défense,
haut fonctionnaire correspondant de
défense et de sécurité adjoint

ORIGINAL SIGNE

LISTE DE DIFFUSION

DESTINATAIRES :

- AMIAD
- DGA (SSDI, SASD, DIE, DOMN)
- DGSE
- CND (GOUV STRAT, SD SEC NUM)
- DRSD
- EMA (COMCYBER, COCA, SNA, FN)
- EMAT
- EMM
- EMAAE
- SGA (DTPM)

COPIES :

- C1
- CM 1
- CM 3
- DPID (FSSI, DSN)
- Archives

DIRECTIVE N°27
PORTANT SUR
L'HOMOLOGATION DES SYSTÈMES D'INFORMATION
DU MINISTÈRE DES ARMÉES

Version 3.1

(approuvée par la note n°DEP-00106/2026/ARM/DPID/NP du 25 février 2026)

Rédaction	ICD Thierry CHATONNET	DPID/DSN
Vérification	AQSSI	EMDS
Vérification	CF Jean-Michel LY SIOU CHING-KERNEIS	DPID/C.DSN
Vérification	ICA Harold HOFF	FSSI du MINARM
Approbation	GDA Nicolas LEVERRIER	DPID

RÉSUMÉ

Compte-tenu de la forte dépendance des missions du ministère aux systèmes d'information (SI) et des menaces toujours plus grandes qui pèsent sur eux, il est obligatoire de les homologuer, y compris ceux qui sont déjà en service.

L'homologation des SI permet d'en connaître le périmètre et l'état de sécurité, d'évaluer les risques qui pèsent sur les capacités opérationnelles auxquelles ces SI contribuent, d'assurer une prise en compte de leurs besoins de sécurité à juste niveau et d'améliorer leur résilience. Elle concourt enfin à maintenir le niveau de sécurité du SI au cours de son utilisation, à résoudre des incidents et à gérer des crises. À noter qu'en cas d'incident sur des SI qui ne disposeraient pas de décisions d'homologation valides, la responsabilité des autorités d'emploi serait directement engagée.

L'édition n°3.1 de la directive 27 rappelle les principes de l'homologation, maintient les trois types de démarches d'homologation (sommaire, simplifiée, standard) et en clarifie les différentes modalités en distinguant davantage les cas d'usage afin de rendre plus rapide et pertinent le processus d'homologation.

Elle insiste notamment sur la nécessité de prendre en compte, dans le processus, le contexte de déploiement du SI afin de garantir le succès de la démarche. Cette édition résulte également d'un retour d'expérience mené dans les armées, directions et services (ADS).

Elle propose en outre certaines mesures techniques devant permettre aux AQSSI d'homologuer plus sans dégrader le niveau de sécurité. Peuvent ainsi être cités :

- **l'allègement** du formalisme par un recours accru à la **dématérialisation** ou à la décision sur dossier,
- l'ouverture de nouvelles possibilités, telles que **l'homologation de SI similaires**, et l'ajout de cas d'usage pour **l'homologation de SI par héritage**,
- la simplification des démarches d'homologation pour les **SI isolés et simples** de niveau Secret,
- la fluidification du processus de **re-homologation**,
- la notion **d'homologation sous réserves** en cas d'urgence politique, stratégique ou opérationnelle.

Elle référence les boîtes à outils mises en œuvre par trois AQSSI : les kits RSSI du COMCYBER et du SGA, ainsi que dans le pack homologation de la DGA (base CASSIS). Enfin, elle tient compte des évolutions de la réglementation, en particulier la dernière version de l'instruction générale interministérielle 1300 sur la protection du secret de la défense nationale du 9 août 2021, ainsi que la directive DGNUM n°47 du 4 juin 2020 portant sur le maintien en condition de sécurité (MCS) des SI du ministère. Elle converge lorsque cela est judicieux vers la nouvelle doctrine d'homologation de l'ANSSI (avril 2025), qui vise à simplifier pour homologuer plus.

Nota :

- les termes entre crochets ([]) figurent dans les documents de référence (cf. [Annexe 5](#)) ;
- Dans ce document, les recommandations organisationnelles sont identifiées par les lettres **RO** ;

Les principales **modifications** du document par rapport à la v3 sont identifiées de cette façon.

TABLE DES MATIÈRES

1. PRÉSENTATION GÉNÉRALE ET GUIDE D'USAGE	5
1.1. Présentation	5
1.2. Champ et modalités d'application	6
1.3. Niveaux de préconisation	7
1.4. Gestion des dérogations aux règles de la directive	7
2. ORGANISATION	8
2.1. Autorité d'emploi	8
2.2. Autorité d'homologation	8
2.2.1. Désignation de l'autorité d'homologation	8
2.2.2. Transfert de responsabilités	9
2.3. Centre expert de l'autorité d'homologation	9
2.4. Responsable SSI du SI	9
2.5. Commission d'homologation	10
3. DÉMARCHE D'HOMOLOGATION	12
3.1. Objectifs	12
3.2. Processus de maîtrise des risques	12
3.3. Méthode d'analyse de risques	14
3.4. Dossier d'homologation	14
3.4.1. Le périmètre d'homologation	14
3.4.2. La stratégie d'homologation	15
3.4.3. Les procédures d'exploitation de sécurité	15
3.4.4. La liste des risques résiduels	16
3.4.5. Le plan de traitement du risque	16
3.5. Trois types de démarche	17
3.5.1. Démarche sommaire	17
3.5.2. Démarche simplifiée	17
3.5.3. Démarche standard	18
3.6. Détermination du choix de la démarche	18
3.7. Principe de l'héritage	20
4. DÉCISION D'HOMOLOGATION	21
4.1. Objectifs	21
4.2. La forme de la décision d'homologation	21
4.3. La durée de validité de la décision d'homologation	22
4.4. Abrogation d'une homologation	23
4.5. Renouvellement des homologations	23
5. CAS D'USAGE	24
5.1. Système d'information d'importance vitale	24

5.1.1.	Démarche d'homologation d'un SIIV	24
5.1.2.	Décision d'homologation d'un SIIV	25
5.2.	Traitement de données classifiées	26
5.3.	Traitement de données à caractère personnel	27
5.5.	Déploiement opérationnel (OPEX, OPINT, exercice, etc.)	29
5.6.	Déploiements successifs d'un même SI	29
5.6.1.	Présentation	29
5.6.2.	Procédure	29
5.6.3.	Homologation de déploiement dérogatoire	30
5.6.4.	Renouvellement de l'homologation	32
5.6.5.	Suspension et abrogation de l'homologation de déploiement	32
5.7.	Homologation de SI similaires	33
5.8.	Homologation de SI hébergés au ministère	33
5.9.	Homologation de SI utilisant un service d'informatique en nuage externalisé	34
5.9.1.	Solution publique de type IaaS ou PaaS	34
5.9.2.	Solution publique de type SaaS	34
5.10.	Homologation de systèmes de systèmes	35
5.11.	Dispositifs d'interconnexion ou d'interface	36
5.11.1.	Homologation spécifique	36
5.11.2.	Désignation de l'autorité d'homologation	36
5.13.	Homologation d'un SI développé en mode agile	37
5.13.1.	Homologation itérative	37
5.13.2.	Décision d'homologation initiale	38
5.13.3.	Au cours du développement	38
5.13.4.	Décision d'homologation ferme	39
5.14.	Cas de mise en exploitation pour test ou expérimentation	39
5.15.	Cas de régularisation	40
5.15.1.	Dossier d'homologation	40
5.15.2.	Démarche d'homologation	40
5.15.3.	Décision d'homologation	41
ANNEXE 1.	LE DOSSIER D'HOMOLOGATION	42
ANNEXE 2.	SCHÉMA DE PRINCIPE DE L'HOMOLOGATION	44
ANNEXE 3.	FORMATION : SAVOIR ET SAVOIR-FAIRE	45
ANNEXE 4.	LISTES DES EXIGENCES	47
ANNEXE 5.	CADRE DOCUMENTAIRE	51

1. PRÉSENTATION GÉNÉRALE ET GUIDE D'USAGE

1.1. Présentation

« L'homologation est obligatoire pour tous les systèmes numériques utilisés ou mis en œuvre par le ministère, par un **établissement public (EP)** sous tutelle et par un **fournisseur** lorsque la réglementation ou son contrat l'y oblige. » [PMSN-S]

Le terme d'homologation de sécurité traite de:

- la démarche d'homologation (cf. §3) ;
- **la décision d'homologation** (cf. §4).

La **démarche d'homologation** vise à obtenir une décision d'homologation, pour cela :

Elle doit être adaptée au système d'information (SI), à son contexte d'emploi, dont les autres SI avec lesquels il est connecté, à la nature des données qu'il traite, aux fonctions opérationnelles auxquelles il contribue directement ou indirectement, tout en prenant en compte l'état de la menace.

- Elle participe et veille au MCS du SI dont les modalités de mise en œuvre sont définies dans la directive [MCS].
- Les travaux menant à l'homologation débutent dès la conception du système d'information et se terminent lors de son décommissionnement.
- Les travaux sont cycliques et itératifs. Chaque fin de cycle fait l'objet d'une décision d'homologation.

La **décision d'homologation** de sécurité d'un SI est l'attestation formelle prise par l'autorité qualifiée en matière de SSI (AQSSI), ou toute autorité d'homologation (AH) qu'elle a formellement désignée (cf. §2.2). Par cette décision, celle-ci :

- s'assure que les risques de sécurité liés à l'utilisation du système d'information ont été identifiés et que les mesures nécessaires pour les traiter sont ou vont être mises en œuvre dans un délai raisonnable ;
- s'assure que les réglementations en vigueur sont correctement appliquées ;
- valide le plan d'actions à appliquer au système d'information afin de renforcer sa sécurité ;
- assume les risques résiduels pesant sur le SI considéré, et donc sur les activités qu'il porte, dans un périmètre d'emploi donné. Dans le cadre d'un système classifié, elle atteste de la capacité de ce système à traiter des informations classifiées pour un niveau de classification donné [IGI 1300].

La présente directive définit les principes et modalités relatifs aux homologations de sécurité des SI au sein du ministère des Armées. Elle tient compte des dispositions de la réglementation en vigueur et des retours d'expérience en matière d'homologation de systèmes nationaux.

Les SI déjà en exploitation, non encore homologués, doivent faire l'objet d'une régularisation

La mise en exploitation d'un système :

- sans décision d'homologation ;
- avant la décision d'homologation ;
- ou hors du périmètre d'homologation défini ;

est un cas de non-respect de la [PMSN-S] et engage directement la responsabilité de l'autorité d'emploi (AE) et éventuellement des opérateurs.

Si les enjeux de sécurité du SI le permettent, des mesures dérogatoires à la démarche d'homologation peuvent être autorisées par l'AQSSI pour faciliter son homologation.

1.2. Champ et modalités d'application

La présente directive est applicable aux organismes du ministère des Armées directement ou par voie de tutelle et, en tant que de besoin, aux prestataires¹. **La directive est applicable aux établissements publics sous tutelle, lorsque le ministère des Armées exerce seul la tutelle, et dans le cas d'une co-tutelle, si le ministère est désigné comme ministère de référence en matière de sécurité numérique, ainsi qu'au CEA/DAM.**

La directive concerne aussi bien les autorités d'emploi (AE) (cf. §2.1), les autorités d'homologation (AH) (cf. §2.2), leur centre d'experts de la SSI (cf. §2.3), les responsables SSI (cf. §2.4) que les officiers et les directeurs de programmes, les responsables de conduite de projet (RCP), les différents acteurs des projets en mode agile et les opérateurs.

La directive ne s'applique pas aux SI interministériels ou mis en œuvre par l'OTAN ou l'UE. Dans ce cas, il convient de se référer aux documents idoines.

L'homologation de sécurité d'un SI est globale : elle inclut dans son périmètre tout ce qui peut impacter la sécurité numérique du système et des données.

Le **[GUIDE 7]** précise les modalités définies dans cette directive et propose des modèles de livrables.. Son usage et sa large diffusion sont donc fortement recommandés. Les modèles dans les kits RSSI du COMCYBER **[KIT RSSI COMCYBER]** du SGA **[KIT RSSI SGA]**, et le pack homologation de la DGA **[BASECASSIS]**.

Cette directive est applicable à partir de sa publication. Cette version annule et remplace la précédente édition (version n°3 du 7 juin 2022).

¹Prestataire au sens de fournisseur lié par accord (contrat direct ou indirect, convention, etc.).

1.3. Niveaux de préconisation

Les règles définies dans ce document ont différents niveaux de préconisation et sont conformes au [RGI] et à la [RFC 2119]² :

OBLIGATOIRE	Ce niveau de préconisation signifie que la règle édictée indique une exigence absolue de la directive.
RECOMMANDÉ	Ce niveau de préconisation signifie qu'il peut exister des raisons valables, dans des circonstances particulières, pour ignorer la règle édictée, mais les conséquences doivent être comprises et pesées soigneusement avant de choisir une voie différente.
CONSEILLÉ	Ce niveau de préconisation signifie que la règle édictée est une bonne pratique de SSI. Il n'est pas nécessaire d'instruire une dérogation lorsqu'elle n'est pas respectée.
DÉCONSEILLÉ	Ce niveau de préconisation signifie que la règle édictée indique une prohibition qu'il est toutefois possible, dans des circonstances particulières, de ne pas suivre, mais les conséquences doivent être comprises et soigneusement pesées.
INTERDIT	Ce niveau de préconisation signifie que la règle édictée indique une prohibition absolue de la directive.

1.4. Gestion des dérogations aux règles de la directive

Les dérogations à des règles de niveau **OBLIGATOIRE** ou **INTERDIT** sont du ressort de l'AQSSI. Le FSSI et le CND en sont tenus informés.

Les dérogations à des règles de niveau **RECOMMANDÉ** ou **DÉCONSEILLÉ** sont du ressort de l'AH. L'AQSSI en est tenue informée.

Les dérogations octroyées sont à lister et à insérer dans le dossier d'homologation.

² <https://www.ietf.org/rfc/rfc2119.txt> – spécification relative aux niveaux d'exigence de l'IETF (Internet Engineering Task Force) qui produit la plupart des standards d'Internet.

2. ORGANISATION

2.1. Autorité d'emploi

L'Autorité d'emploi (AE) veille :

- à la prise en compte de ses besoins de sécurité dans la conception et l'exploitation de ses SI et dans le traitement de ses données ;
- à la cohérence des mesures mises en place dans ses SI avec ses besoins métiers ou opérationnels et avec les risques en matière de sécurité numérique.

Elle s'assure que :

- tous les SI qui relèvent de sa responsabilité sont homologués ou font l'objet d'une démarche d'homologation ou de ré-homologation ;
- les conditions de leur homologation et les restrictions d'emploi décidées par l'AH, si elles sont définies, sont respectées ;
- les besoins métiers ou opérationnels dans les contextes d'emploi de ses SI, c'est-à-dire les fonctions et données métiers, les conditions d'exploitation et les enjeux métiers ou opérationnels, sont bien pris en compte dans leur démarche d'homologation ;
- les mesures de continuité d'activité et de reprise d'activité sont adaptées aux risques résiduels validés par l'AH.

L'AE du SI doit obligatoirement prendre en compte la décision de l'AH avant de décider sa première mise en exploitation, y compris dans un cadre d'expérimentation. Idéalement, la décision d'homologation et la décision de mise en service opérationnel devraient être portées par la même autorité.

En cas d'absence de décision d'homologation pour un SI en utilisation, l'AE assume la responsabilité, notamment pénale, des conséquences de tout événement de sécurité numérique survenant sur le SI. La responsabilité des entités utilisatrices, ainsi que celle de l'autorité en charge de son exploitation technique, peuvent aussi être engagées.

2.2. Autorité d'homologation

2.2.1. *Désignation de l'autorité d'homologation*

L'autorité d'homologation (AH) est l'autorité à qui l'AQSSI délègue tout ou partie de ses attributions relatives à la démarche d'homologation de la **[PMSN-S]**. Les règles de délégation sont fixées par l'AQSSI qui en précise les conditions (attributions, périmètre de dérogation, niveau de confidentialité maximal, activité d'application, possibilité éventuelle de subdélégation).

Pour porter les responsabilités d'AH, l'autorité doit maîtriser le besoin métier ou opérationnel, disposer des moyens de maîtriser le risque en matière de sécurité numérique ou, à défaut solliciter les ressources pour ce faire. Toutefois, l'AQSSI est responsable des ressources à affecter à la mise en œuvre de la démarche d'homologation.

- RO 1 :** il est **OBLIGATOIRE** que tout SI du ministère, pour un périmètre d'homologation donné, dispose d'une seule AH formellement désignée.
- RO 2 :** il est **RECOMMANDÉ** que l'AH soit désignée au sein de la chaîne d'emploi du SI.

2.2.2. Transfert de responsabilités

Au cours de son cycle de vie, l'homologation d'un SI, pour un périmètre donné, peut être réattribuée à une nouvelle AH lorsque l'AQSSI le décide ou lorsque le SI n'est plus dans le périmètre de l'AQSSI **d'origine (notamment quand le SI est transféré vers une autre AE, ou encore suite à une réorganisation structurelle ou à une évolution majeure du SI).**

RO 3 : il est **OBLIGATOIRE**, en cas de changement d'AH au cours du cycle de vie du SI, de procéder formellement à un transfert de responsabilités au cours duquel le dossier d'homologation du SI est transmis à la nouvelle AH.

Si le besoin est exprimé par l'une des AH, le transfert de responsabilités peut avoir lieu à l'issue d'une réunion formelle présidée par le représentant de l'AQSSI, ou co-présidée par les AQSSI sortante et prenante en cas de changement d'AQSSI. Cette réunion est composée au minimum des AE et des AH concernées (prenantes et si possible sortantes) ainsi que d'un représentant de leur centre expert. Le FSSI peut y participer. Les risques résiduels sont présentés au cours de la réunion. La réunion donne lieu à un procès-verbal qui mentionne notamment les remarques et restrictions de la partie prenante.

Une décision formelle notifie les nouvelles responsabilités, celle-ci est émise par l'AH prenante vers l'AQSSI, l'AH sortante, et le FSSI. La responsabilité de l'AH sortante est pleine et entière jusqu'à sa parution.

Si les risques résiduels, les conditions de MCS et le niveau de sécurité du SI ne sont pas acceptables pour l'AH prenante, celle-ci mettra en œuvre une nouvelle démarche d'homologation.

RO 4 : il est **OBLIGATOIRE** de renouveler la décision d'homologation en cas de transfert de responsabilité d'AH. La mise en œuvre de ce renouvellement est laissée à l'appréciation de l'AH prenante **dans un délai maximal d'un an.**

Le transfert de responsabilités est effectif dès validation de la décision d'homologation par la nouvelle AH.

2.3. Centre expert de l'autorité d'homologation

L'AH s'appuie sur un centre d'experts en SSI, dit **centre expert de l'AH (CEAH)**, qui suit les démarches d'homologation, vérifie le dossier d'homologation et prépare ses décisions. Il apporte son appui et son expertise auprès des responsables SSI (RSSI) des SI qui relèvent de son périmètre de responsabilités.

RO 5 : il est **OBLIGATOIRE** pour une AH de disposer d'au moins un spécialiste en sécurité du numérique formé à la démarche d'homologation.

L'annexe 3 propose une liste de connaissances et de compétences qu'il convient de détenir pour mener des démarches d'homologation.

2.4. Responsable SSI du SI

Le Responsable SSI projet (RSSI-P) conduit la démarche d'homologation sous la responsabilité de l'AE et au profit du responsable de projet (RCP) ou de programme jusqu'à la première décision d'homologation, et tant que le SI est en phase de conception ou de réalisation.

Le RSSI aval (RSSI-A) conduit les démarches d'homologation lorsque le SI n'est plus en phase de réalisation pour renouveler la décision d'homologation, et ceci sous la responsabilité de l'AE.

Si le SI n'est pas homologué alors qu'il est déjà en phase d'utilisation, il instruit une démarche d'homologation pour régularisation.

Les fonctions de RSSI-P et de RSSI-A peuvent ne pas être distinctes et être portées par un seul RSSI³.

En absence de RSSI, un SI ne peut être homologué ou ré-homologué, et en cas de SI déjà homologué, la décision d'homologation peut être remise en cause. Il est de la responsabilité de l'AE de s'assurer de la continuité de la fonction de RSSI tout au long du cycle de vie du SI.

Le transfert de la fonction de RSSI, notamment de la fonction de RSSI-P à celle de RSSI-A en cas d'attributaires différents, requiert au minimum :

- un transfert du dossier d'homologation du SI réactualisé, contenant notamment le plan de traitement des risques (PTR, cf. §3.4.5) ;
- une désignation formelle du RSSI prenant et de la date effective de sa prise de fonction.

Le transfert de responsabilité nécessite un procès-verbal qui définit les pièces transmises, les remarques et les restrictions du RSSI prenant. Il est transmis à l'AE et à l'AH.

2.5. Commission d'homologation

La commission d'homologation est une instance mise en place pour informer et conseiller l'AH au moment de décider de l'homologation du SI. Le FSSI, l'AQSSI et l'**OSSI de chaîne ou leur représentant sont membres de droit des commissions d'homologation**. Ils sont informés de leur tenue et ils peuvent accéder à l'ensemble du dossier d'homologation.

RO 6 : il est **OBLIGATOIRE** que l'AH constitue une commission d'homologation, adaptée au système à homologuer et en fixe les règles générales de fonctionnement.

³ Dans la présente directive, le terme de RSSI désigne les deux fonctions, RSSI-P et RSSI-A, qui se distinguent selon la phase du cycle de vie du SI.

Après validation par le CEAH du dossier d'homologation constitué par le RSSI, les membres de la commission sont appelés à se prononcer afin de proposer à l'AH une décision d'homologation. Cette dernière sera formalisée au travers d'un procès-verbal de réunion, d'une note de service ou d'un message officiel (NEMO). La composition de cette commission dépend de l'enjeu et de la nature de l'homologation. Dans les cas les plus simples (démarche sommaire (cf. §3.5.1), simplifiée (cf. §3.5.2), homologation de déploiement (cf. §5.6) par exemple), la composition de la commission reste à la diligence de l'AH. Elle peut se limiter au CEAH et au RSSI en charge de la démarche d'homologation. Un certificat de conformité aux exigences SSI peut faire office de procès-verbal.

Sur proposition du CEAH, l'autorité d'homologation peut décider d'arrêter sa décision sur la base du dossier fourni, sans nécessairement réunir physiquement les membres de la commission. En tel cas, les avis des parties prenantes devront être collectés par écrit par le CEAH lors de sollicitations préalables.

Cette disposition n'est pas applicable pour les SI du contrôle gouvernemental, ni pour les SIIV.

RO 7 : il est **OBLIGATOIRE** que l'AH constitue une commission d'homologation, adaptée au système à homologuer et en fixe les règles générales de fonctionnement. il est **OBLIGATOIRE** que, dans le cadre d'une démarche d'homologation standard, la commission d'homologation soit au minimum composée des acteurs suivants :

- l'AH ou son représentant ;
- le responsable SSI (RSSI) en charge de la démarche d'homologation ;
- le responsable de projet (RCP ou équivalent)/programme ou son représentant ;
- l'AE ou son représentant.

Dans le cas d'un renouvellement d'une homologation (cf. §4.5), la constitution de la commission d'homologation est à la diligence de l'AH. La commission doit au moins comprendre :

- le CEAH ;
- le RSSI en charge de la démarche de renouvellement de l'homologation ;
- le RSSI (ou RSSI-A) du SI (s'il est différent du RSSI en charge de la démarche d'homologation) ;
- le responsable du MCS (s'il est différent du RSSI).

Dans le cadre d'une régularisation d'une homologation d'un SI déjà en phase d'utilisation, la commission comprend au moins :

- l'AH ou son représentant ;
- le RSSI en charge de la démarche d'homologation ;
- le RSSI-A du SI (s'il est différent du RSSI en charge de la démarche d'homologation) ;
- le représentant de l'opérateur ;
- l'AE ou son représentant.

3. DÉMARCHE D'HOMOLOGATION

3.1. Objectifs

La démarche d'homologation a pour objectif :

- d'une part :
 - o d'identifier, d'évaluer et de hiérarchiser les risques résiduels portant sur le SI dans un périmètre bien défini selon les principes de gestion de risques ;
 - o de réduire la vraisemblance des risques, en particulier la surface d'attaque, ou le cas échéant leurs impacts, par l'application de mesures de sécurité ;
 - o de mettre en place la capacité à réagir en cas d'incident ou de crise ;
 - o de s'assurer de l'effectivité des règles relatives au **[MCS]** et aux **[Traces]** ;
- d'autre part :
 - o de justifier le bon déroulement de la démarche ;
 - o de fournir à l'AH les justifications nécessaires pour prononcer sa décision.

La démarche d'homologation doit amener à une décision d'homologation (cf. §4).

3.2. Processus de maîtrise des risques

L'AH décide des modalités de la démarche et peut la faire évoluer en conduite.

Toutefois, la démarche d'homologation doit être adaptée en termes de :

- **méthode**, aux enjeux portés par le SI en termes de niveau de risque et de ressources tout au long de son cycle de vie ;
- **mesures de sécurité**, pour éviter d'entraver le développement du SI par la « sur-sécurité » ;
- **documentation**, pour ne pas multiplier les livrables fastidieux, inadaptés ou encore inefficaces.

Il s'agit donc de **prioriser les démarches d'homologation en fonction du niveau de criticité des SI et de leur exposition aux menaces** afin d'éviter d'instruire des processus d'homologation complexes, longs et coûteux qui finalement seraient inadaptés aux enjeux de sécurité des SI.

Toute démarche d'homologation repose sur un **processus de maîtrise des risques** qui se déroule en plusieurs étapes :

- définition du périmètre d'homologation (cf. §3.4.1) ;
- description de la démarche dans une stratégie d'homologation (cf. §3.4.2) ;
- définition des objectifs de sécurité ;
- identification, évaluation et hiérarchisation des risques portés sur le SI au moyen d'une analyse de risques ou de conformité à un référentiel préalablement défini (cf. RO 8 : ci-dessous) ;
- traitement des risques hiérarchisés ;
- réalisation et contrôle des mesures de sécurité destinées à atteindre les objectifs de sécurité ;
- identification, évaluation et hiérarchisation des risques résiduels ;
- constitution et vérification du dossier d'homologation (cf. §3.4) ;
- décision de l'AH (cf. §4) sur avis de la commission d'homologation (cf. §2.5).

Lors de la démarche d'homologation, le RSSI doit tenir compte au minimum :

- des attendus métiers (AE) ;
- du fondement juridique et réglementaire s'appliquant à la protection des données et des SI ;
- des prérequis nécessaires à l'homologation (par exemple, la qualification de produits de sécurité) ;
- de l'interconnexion avec d'autres systèmes ;
- du réseau utilisé ;
- des moyens d'hébergement des informations ;
- des solutions de chiffrement (logicielles et matérielles) ;
- de la gestion des documentations, notamment de la cartographie afin de garantir la connaissance du système au cours de son cycle de vie ;
- de la gestion et de la protection des supports amovibles ;
- des accès à distance par des utilisateurs en mobilité ;
- de la pile applicative ;
- des conditions de MCS conformément au **[MCS]** ou à ses déclinaisons au sein des ADS ;
- des modalités de supervision de sécurité ;
- des opérations de maintenance, d'exploitation ou de télégestion du système, notamment lorsqu'elles sont effectuées par des prestataires externes ;
- des éléments mis en œuvre pour assurer le plan de continuité/reprise d'activité (PCA/PRA) ;
- de la formation des utilisateurs et des administrateurs, y compris sur la sécurité ;
- des contraintes et des impératifs, notamment calendaires ;
- des modalités de retrait de service.

Le niveau de supervision du système doit être pris en compte dans la démarche d'homologation conformément aux recommandations de l'ANSSI et du COMCYBER. Celui-ci doit être instruit suffisamment tôt dans la réalisation du SI afin de prendre en compte les prérequis et prévoir d'intégrer le cas échéant cette mise sous supervision dans le plan de charge du SOC.

RO 8 : il est **OBLIGATOIRE** de renseigner les informations relatives à la démarche d'homologation dans l'outil de suivi du patrimoine applicatif du ministère des Armées⁴ et de les réactualiser au fur et à mesure de la démarche d'homologation (sous réserve du niveau de classification de ces informations).

⁴ SICLADE est l'outil de suivi du patrimoine applicatif du ministère des Armées.

3.3. Méthode d'analyse de risques

La méthode d'analyse de risques à utiliser est **[EBIOS RM]**. D'autres méthodes peuvent être utilisées en complément sur autorisation de l'AH (cf. **[PSSIM-T]** ENV13). Dans ce cas, il est nécessaire de le préciser et de le justifier dans la stratégie d'homologation.

3.4. Dossier d'homologation

L'AH doit s'appuyer sur les livrables produits par la démarche d'homologation pour prononcer la décision d'homologation. L'ensemble des livrables constitue le dossier d'homologation.

RO 9 : il est **OBLIGATOIRE**, afin que la décision d'homologation soit motivée et justifiée, que l'AH s'appuie sur un dossier d'homologation conforme à la démarche d'homologation choisie et dont les pièces constitutives sont définies par la stratégie d'homologation

Quelle que soit la démarche d'homologation, le dossier d'homologation est **a minima** constitué des éléments suivants :

- **la stratégie d'homologation**, pièce maîtresse de la démarche, qui définit le périmètre d'homologation et qui identifie les responsabilités, les tâches à réaliser (éventuellement assorties de conditions), ainsi que les livrables à fournir (cf. §3.4.2) ;
- **les procédures d'exploitation de sécurité** (PES) qui précisent les mesures organisationnelles de sécurité à appliquer au SI (cf. §3.4.3) ;
- **la liste des risques résiduels** portant sur le SI (cf. §3.4.4) ;
- le plan de traitement des risques (cf. §4.4.5).

Si la mise sous supervision de sécurité du SI par un SOC est décidée, la démarche d'homologation doit vérifier que les prérequis nécessaires à cette mise sous supervision ont bien été pris en compte. Le SOC peut fournir un compte-rendu de faisabilité qui sera alors inséré dans le dossier d'homologation.

Dans le cas d'une prestation informatique confiée à un tiers externe au ministère, notamment une prestation d'hébergement, le dossier d'homologation doit comprendre un plan d'assurance de sécurité (PAS) produit par le prestataire accompagné d'un certificat attestant de sa conformité.

RO 10 : il est **OBLIGATOIRE** pour le RSSI de constituer le dossier d'homologation tel qu'il est défini dans la stratégie d'homologation et de le faire valider par le CEAH.

Par sa validation, le CEAH atteste que le dossier d'homologation est conforme aux attendus de la stratégie d'homologation approuvée par l'AH. Il prononce un avis sur sa complétude et sur le contenu des pièces le constituant.

L'approbation et la validation d'un dossier d'homologation impliquent l'approbation et la validation de toutes les pièces qui le constituent.

Le dossier d'homologation, initié dès la phase de conception du SI, est tenu à jour tout au long du cycle de vie du SI. Il est **revu et contrôlé à chaque renouvellement d'homologation et à chaque changement de RSSI**.

3.4.1. *Le périmètre d'homologation*

RO 11 : il est **OBLIGATOIRE** pour le RSSI de documenter le périmètre d'homologation, validé par l'AH, et de l'actualiser au fur et à mesure de l'évolution du SI.

Le périmètre d'homologation précise *a minima* les éléments suivants au fur et à mesure du projet :

- les différents contextes d'emploi possibles du SI ;
- les enjeux et les besoins de sécurité exprimés par l'AE ;
- les acteurs du SI (AE, opérateur, organisme utilisateur, etc.) ;
- les principales fonctionnalités du SI ou cas d'usage ;
- la nature des données traitées par le SI, notamment leur niveau de confidentialité ;
- les différents profils d'utilisateurs ;
- la configuration technique du SI ;
- les dispositifs d'échanges, d'interconnexion et d'interfaces avec d'autres SI ;
- les références relatives au SI ayant un impact sur la sécurité numérique et la démarche d'homologation (CCTP, contrat MCO/MCS, contrat d'hébergement, etc.).

En raison de son usage récurrent dans différents livrables et de ses possibles évolutions, le périmètre d'homologation peut faire l'objet d'un document de référence. Il est alors joint à la stratégie d'homologation ou à tout document le nécessitant.

3.4.2. La stratégie d'homologation

RO 12 : il est **OBLIGATOIRE** pour le RSSI d'établir une stratégie d'homologation, puis de la faire approuver par l'AH.

La stratégie d'homologation précise *a minima* les informations suivantes :

- le périmètre d'homologation (ou référence du document définissant ce périmètre) ;
- les acteurs de la démarche d'homologation ;
- le référentiel réglementaire ;
- le type de démarche d'homologation (cf. §4.5) ;
- les analyses de risques à réaliser et les méthodes à employer ;
- le parcours (séquences, cas d'usage traités) de l'homologation à instruire ;
- les éléments de la stratégie de MCS du SI ;
- les modalités de mise sous supervision de sécurité⁵ ;
- les livrables à produire avec les responsabilités, les échéances et les approbateurs ;
- les modalités de la commission d'homologation (composition, nature de la réunion) ;
- les contraintes et les impératifs, notamment calendaires.

3.4.3. Les procédures d'exploitation de sécurité

RO 13 : il est **OBLIGATOIRE** pour le RSSI de rédiger des PES et de les faire approuver par l'AH, après accord de l'AE.

Les PES définissent *a minima* :

- les différentes responsabilités des acteurs en matière de SSI et d'exploitation ;

⁵ Par un SOC, une surveillance périodique des journaux, etc.

- les mesures organisationnelles de sécurité spécifiques au SI, dont nécessairement :
 - o la gestion des accès et des droits ;
 - o l'organisation du MCS ;
 - o la supervision de sécurité (stratégie de détection, politique de journalisation, etc.) ;
 - o les modalités de sauvegarde et de restauration ;
- les mesures dérogatoires à des exigences de sécurité ;
- les mesures conservatoires, notamment à des fins pédagogiques ;
- les limitations d'utilisation du SI ;
- les modalités de retrait de service du SI en matière de sécurité numérique.

Les PES doivent :

- **être adaptées au public visé** (RSSI, administrateurs, utilisateurs)⁶ ;
- ne contenir que les informations strictement nécessaires aux destinataires.

3.4.4. La liste des risques résiduels

L'ensemble des risques portant sur le SI et subsistant toujours après l'implémentation des mesures de sécurité doit être présenté à l'AH avec les niveaux de gravité et de vraisemblance.

Le SI est soumis à un ensemble d'exigences de sécurité de niveaux d'importance variés en raison de la nature de ses données, des activités qu'il porte ou des éléments qui le constituent. Ces exigences sont extraites d'un référentiel préalablement défini. Lorsque des exigences ne sont pas applicables pour des raisons justifiées, des mesures sont définies pour réduire les risques que cette non-conformité peut générer. **La liste des risques résiduels prend aussi en compte les risques subsistant après la mise en place de ces mesures dérogatoires.**

RO 14 : il est **OBLIGATOIRE** pour l'AH de délivrer une décision d'homologation à partir d'une liste de risques résiduels après avoir autorisé les mesures dérogatoires relevant de son périmètre.

3.4.5. Le plan de traitement du risque

Le **plan de traitement du risque (PTR)** définit et suit dans le temps les mesures de sécurité à appliquer à un SI pour réduire les risques, traiter les non-conformités et les vulnérabilités du SI.

- Le **PTR** identifie le responsable de chaque mesure et les difficultés de mise en œuvre, évalue le coût nécessaire pour la réaliser, son échéance et son état de réalisation. Chaque mesure est associée à au moins un risque.

RO 15 : il est **OBLIGATOIRE** pour l'AH de valider un plan de traitement du risque (PTR), celui-ci est initié et mis à jour par le RSSI dès la phase de développement du SI et tout au long du cycle de vie

⁶ Des PES peuvent en annexe fournir des fiches réflexes par public visé.

3.5. Trois types de démarche

La présente directive définit trois types de démarche d'homologation : sommaire, simplifiée et standard.

Les types de démarche d'homologation se différencient par :

- la nature et la profondeur de l'analyse de risques (cf. **Erreur ! Source du renvoi introuvable.**) ;
- la composition du dossier d'homologation (cf. ANNEXE 1) ;
- la composition de la commission d'homologation.

RO 16 : il est **OBLIGATOIRE**, pour homologuer un SI, d'appliquer l'une des trois démarches d'homologation identifiées : sommaire, simplifiée ou standard.

3.5.1. *Démarche sommaire*

La démarche sommaire repose sur une analyse de risques réalisée à partir d'un **certificat d'usage et de conformité (CUC)** fondé sur le **[GUIDE SSI]**, éventuellement complété par la **[PMSN-S]**, les politiques de sécurité du SI qui l'héberge, voire de la **[DIR 39]** lorsqu'elle s'applique.

Le **[GUIDE 7]** propose un modèle de CUC à adapter par les AH.

RO 17 : il est **OBLIGATOIRE** pour l'AH, dans une démarche sommaire, de fournir au RSSI le CUC qu'il devra renseigner. Le CUC sera ensuite soumis à la validation de l'AE.

3.5.2. *Démarche simplifiée*

La démarche simplifiée repose sur une analyse de conformité à un ensemble d'exigences de sécurité vérifiables, déterminées en fonction de la nature des données traitées par le SI, des activités qu'il porte ou encore des éléments (techniques, logiciels) qui le constituent. Il regroupe ainsi un ensemble de règles provenant de textes réglementaires, de normes et de bonnes pratiques préalablement définies, adaptées et applicables au SI. Cet ensemble d'exigences de sécurité à appliquer, associées à leur référentiel, constitue **le CUC** spécifique au périmètre d'homologation du SI.

L'analyse de conformité consiste alors à évaluer l'état d'application des exigences, puis à identifier et justifier les écarts. Le CUC correctement renseigné forme **le socle de sécurité du SI**. Des mesures de sécurité dérogatoires peuvent être définies, puis autorisées par l'autorité compétente pour limiter les risques que font peser les non-conformités sur le SI. Elles complètent alors le socle de sécurité.

Si le référentiel et les exigences de sécurité sont insuffisants pour prendre en compte tout le périmètre d'homologation et les besoins de sécurité du SI, l'analyse de conformité devrait être complétée par une analyse de risques appropriée. Cette analyse de risques complémentaire à l'analyse de conformité peut aussi être exigée par l'AH. **Alternativement, la conformité peut être justifiée par les livrables des ateliers 1 et 5 de la méthode EBIOS-RM.**

RO 18 : il est **OBLIGATOIRE**, pour une démarche simplifiée, de procéder à une analyse de conformité à partir d'un CUC, formé d'exigences adaptées au périmètre d'homologation et aux besoins de sécurité du SI (socle de sécurité), **ou, alternativement, de procéder aux ateliers 1 et 5 de la méthode EBIOS-RM.**

RO 19 : il est **RECOMMANDÉ**, pour une démarche simplifiée, de compléter l'analyse de conformité par une analyse de risques **lorsque le CUC est insuffisant** pour prendre en compte les composants essentiels du périmètre d'homologation ou encore les besoins de sécurité du SI.

Un outil d'analyse de risques dédié à la démarche d'homologation simplifiée (OARDHS du **[GUIDE 7]**) pour un SI non industriel est fourni.

3.5.3. Démarche standard

La démarche standard s'appuie obligatoirement sur une analyse de risques complète selon la méthode préconisée par le ministère (**[EBIOS RM]**).

RO 20 : il est **OBLIGATOIRE**, pour une démarche standard, de mener une analyse de risques complète selon la méthode préconisée par le ministère.

L'analyse de risques donne alors lieu à l'élaboration des livrables suivants :

- une **cible de sécurité**, éventuellement. Elle identifie les fonctions de sécurité réalisant les objectifs de sécurité ;
- un **plan de sécurité** (PDS). Il regroupe l'ensemble des mesures organisationnelles, physiques et techniques qui réalisent les fonctions de sécurité prévues ou encore les objectifs de sécurité définis

La cible de sécurité et le PDS permettent de vérifier le recouvrement de l'ensemble des objectifs de sécurité. La cible de sécurité peut être incluse dans le PDS pour former un seul livrable.

Le SI fait l'objet d'un audit (**[Audit]**). Cet audit donne lieu à un rapport qui définit les vulnérabilités identifiées et les risques associés, puis à un plan d'actions.

RO 21 : il est **OBLIGATOIRE**, dans toute démarche standard, de réaliser un audit. Les résultats et les actions qui en découlent sont étudiés lors de la commission d'homologation.

3.6. Détermination du choix de la démarche

Les SI sont répartis en quatre catégories en fonction de la sensibilité et de l'exposition à la menace **[PSSIM-T]** :

- SI d'importance vitale (SIIV) ;
- SI essentiel (SIE) ;
- SI important (SII) ;
- SI standard (SIS).

Les SI industriels font aussi l'objet d'une classification (classes 1 à 3) dont le niveau détermine les mesures de sécurité à appliquer sur un périmètre bien défini (**[DIR 39]**). La catégorisation d'un système industriel peut se déduire de son niveau de classe.

L'AH valide la catégorisation du SI, sur proposition de l'autorité d'emploi, au regard de l'importance du SI pour le fonctionnement de l'entité ou la réalisation de la mission, et de l'exposition aux menaces. L'AE est assistée par sa chaîne fonctionnelle SSI.

Le choix du type de démarche d'homologation doit être en accord avec la catégorisation du SI. Typiquement, les correspondances suivantes peuvent être appliquées.

	Système d'information	Système industriel (ou sous-système)
Démarche standard	SIIV	
	SIE	classe 3
Démarche simplifiée	SII	classe 2
Démarche sommaire	SIS	classe 1

Tableau 1. Choix du type d'homologation selon le type de SI

La **complexité du SI**, et donc de sa maîtrise, peut aussi être un critère supplémentaire dans le choix de la démarche.

La **démarche sommaire** peut correspondre à un SI d'architecture simple, dont l'exposition aux risques **et** la criticité sont faibles et dont les règles de sécurité à appliquer n'excèdent pas celles prévues par les **[GUIDE SSI]**.

La **démarche simplifiée** peut correspondre à un SI d'architecture maîtrisée **et** dont l'exposition aux risques **ou** la criticité est faible. Elle répond notamment au cas des SI s'appuyant sur un socle au travers des usages, ou pouvant faire l'objet d'exigences de sécurité non couvertes par le socle ou par les **[GUIDE SSI]**, mais encadrées par des réglementations relatives aux informations et fonctions à protéger (personnelles, médicales, financières, systèmes industriels, etc.).

La **démarche standard** s'applique aux autres SI, notamment à des SI dont l'exposition aux risques n'est pas maîtrisée au travers du socle **ou** dont les exigences de sécurité ne sont pas couvertes par des réglementations. Elle s'applique principalement à des SI du socle, des SI constituant leur propre socle (par exemple, les systèmes embarqués, les systèmes d'armes, etc.), des SI présentant un fort niveau de criticité (un ou plusieurs critères de risques (DICT⁷) au niveau maximum).

Pour les systèmes non industriels, l'AH pourra s'appuyer sur le questionnaire d'évaluation initiale (QEI) proposé par le **[GUIDE 7]** pour orienter ses choix. Pour les systèmes industriels, une méthode et des outils sont proposés dans la **[DIR 39]**. **Toutefois, l'AH reste seule décisionnaire du choix de la démarche, hormis pour les SI pour lesquels la réglementation et la présente directive peuvent imposer une démarche standard (RGS, SIIV).**

⁷ Disponibilité, Intégrité, Confidentialité, Traçabilité

3.7. Principe de l'héritage⁸

Dans le cadre des homologations, certains systèmes peuvent bénéficier du principe d'héritage de sécurité. Ce dernier regroupe plusieurs cas d'usage :

Les composants ou services bénéficiant d'une qualification ou certification de l'ANSSI

Les SI⁹ dont la sécurité est portée entièrement par un SI d'accueil. Les SI concernés ne peuvent écrire dans le service d'annuaire, ne reçoivent ni n'émettent de flux en dehors du SI d'accueil ;

Les extensions de SI n'entraînant pas d'évolution significative du périmètre du SI, ni de nouveau risque systémique de sécurité.

Dans ces cas de figure et à condition que le nouveau SI n'ajoute aucun risque supplémentaire, sa sécurité est héritée d'un système déjà homologué.

Le principe d'héritage consiste à utiliser les résultats d'une analyse de risques déjà conduite sur un modèle. Celui-ci peut désigner un composant (physique, logiciel), un service, voire une architecture type.

Un modèle est constitué :

- d'une description permettant de l'identifier clairement ;
- d'un niveau de sécurité défini comme l'ensemble des résultats de l'analyse de risques sous forme de critères de sécurité (DICT, etc.) et des risques résiduels ;
- de prérequis sous forme de recueil d'exigences vérifiables.

Tout modèle doit être validé par le RSSI concerné et le CEAH.

L'objet hérite d'un modèle quand il utilise les éléments constituant ce modèle pour identifier, évaluer et hiérarchiser les risques portant sur le SI.

Les risques¹⁰ associés à l'objet qui hérite doivent alors être évalués à partir :

- du niveau de sécurité du modèle hérité ;
- de l'état de conformité du SI au prérequis.

Les modèles hérités, ainsi que l'évaluation des risques associés aux objets qui héritent, sont insérés dans le dossier d'homologation.

⁸ Le principe d'héritage est implicitement utilisé pour les composants ou services certifiés ou labellisés. Le modèle est alors défini par le certificat et le rapport de certification.

⁹ Le modèle correspond alors au SI d'accueil.

¹⁰ Dans le cadre de la méthode **[EBIOS RM]**, le composant ou le service du SI qui hérite est alors considéré comme une partie prenante du SI dont le niveau de confiance ou de menace est évalué à partir des besoins atteints par le modèle, des résultats de l'analyse de risques et de l'état de conformité du SI aux prérequis.

4. DÉCISION D'HOMOLOGATION

4.1. Objectifs

La décision d'homologation est l'acte officiel par lequel l'AH atteste que :

- les risques résiduels sont bien identifiés, évalués et acceptés ;
- les ressources affectées à la démarche d'homologation sont en adéquation avec les enjeux portés par le SI ;
- le dossier d'homologation est satisfaisant et a fait l'objet d'une validation par le CEAH (cf. §3.4) ;
- les mesures annoncées dans le dossier d'homologation sont effectives ou le seront au terme de la réalisation du PTR dont la complétude devra être vérifiée par le RSSI ;
- les solutions de chiffrement font l'objet d'un dossier cryptographique valide¹¹ et leurs risques résiduels sont intégrés dans la liste des risques acceptés ;
- les moyens nécessaires au MCS sont en place, notamment :
 - o une organisation de gestion du SI pérenne et documentée ;
 - o l'effectivité des contrats de MCS ;
 - o une stratégie de MCS mise en œuvre et adaptée à la criticité du SI et à ses contraintes ;
- la supervision de la sécurité répond aux besoins de sécurité du SI et sa mise en supervision par un SOC, si elle a été décidée, est réalisable ;
- les règles relatives à la défendabilité du SI sont appliquées ([DEFEND]) ;
- le SI est enrôlé dans l'outil de suivi du patrimoine applicatif du ministère des Armées.

Une décision d'homologation est nécessairement associée à un périmètre d'homologation.

La qualification, la certification ou l'agrément d'un équipement ne vaut pas homologation. Néanmoins, l'AH peut et doit s'appuyer sur les conditions de la qualification, de la certification ou de l'agrément pour établir sa décision d'homologation dans le périmètre d'emploi qui y est associé.

Avant toute décision d'homologation, le CEAH vérifie que le SI est enrôlé dans l'outil de suivi du patrimoine applicatif du ministère des Armées et auprès d'un SOC pour la gestion et l'exploitation des traces si ce besoin est avéré.

RO 22 : il est **OBLIGATOIRE** d'insérer la décision d'homologation dans l'outil de suivi du patrimoine applicatif du ministère des Armées (sous réserve du niveau de classification de cette décision).

4.2. La forme de la décision d'homologation

Lors de l'instruction d'un dossier d'homologation, il peut être constaté qu'un système ne remplit pas toutes les conditions requises pour son homologation. L'AH peut apprécier les risques pris en cas de mise en exploitation du système pour une durée ou un périmètre limités et les considérer comme acceptables. Dans ce cas, elle peut alors prononcer **une homologation d'une courte durée**¹² (restriction temporelle), et/ou **sur un périmètre réduit** (restriction fonctionnelle), et **assortie d'une**

¹¹ Un dossier cryptographique a pour but de faciliter et de tracer l'expression de besoin capacitaire en solutions de chiffrement, selon le modèle en vigueur. La durée de l'homologation doit être en cohérence avec la validité d'autorisation d'usage des solutions de chiffrement utilisées.

¹² La durée de validité est inférieure à celle prescrite dans le §4.3.

correction des éléments constatés. L'AH doit alors indiquer ses attentes pour éventuellement procéder au renouvellement de l'homologation limitée ou à une homologation ferme, c'est-à-dire pleine et entière.

RO 23 : il est **OBLIGATOIRE** que toute décision d'homologation soit prise à l'issue d'une démarche d'homologation. La décision peut être assortie de conditions ou de restrictions d'emploi (temporelles, fonctionnelles) pour une durée déterminée. La démarche peut aussi conduire à un refus d'homologation.

Une décision d'homologation conditionnelle ou restrictive doit préciser les critères ou les actions nécessaires pour procéder à une homologation ferme. Les actions à réaliser complètent le PTR du SI. Il sera inséré dans le dossier d'homologation et mis à jour tout le long du cycle de vie du SI.

RO 24 : il est **OBLIGATOIRE** d'insérer dans la décision d'homologation le niveau de protection maximal des données pouvant être traitées par le SI et leurs éventuelles mentions de manipulation ou de diffusion.

La mise en service ou le maintien en service d'un SI malgré un refus d'homologation engage directement la responsabilité de l'AE et éventuellement celle des opérateurs. L'AH les informe des risques encourus et de leurs responsabilités.

4.3. La durée de validité de la décision d'homologation

RO 25 : il est **OBLIGATOIRE** d'assortir la décision d'homologation d'une durée de validité et de fixer les conditions de validité.

La durée de validité d'une décision d'homologation est laissée à l'appréciation de l'AH. Toutefois, elle ne doit pas dépasser :

- 2 ans pour les systèmes traitant des informations au moins de niveau de classification TRÈS SECRET ;
- 3 ans pour les systèmes traitant des informations de niveau de classification SECRET ;
- 5 ans pour des systèmes traitant des informations sensibles, y compris celles portant la mention DIFFUSION RESTREINTE ;
- 7 ans pour les autres systèmes.

Dans le cas de systèmes industriels traitant des informations non classifiées, la durée de validité de l'homologation doit être inférieure ou égale à :

- 3 ans pour les SI de classe 3 ;
- 5 ans pour les SI de classe 2 ;
- 7 ans pour les SI de classe 1.

Au-delà de sa date de validité et jusqu'au renouvellement de la décision d'homologation, l'utilisation du SI doit être suspendue.

RO 26 : il est **OBLIGATOIRE** de remettre en cause une décision d'homologation quand :

- les conditions de sa validité ne sont plus respectées ;
- les conditions de configuration ou d'exploitation du SI ont été modifiées de manière significative ;
- le SI ne correspond plus au périmètre d'homologation (ajout de fonctionnalités, d'applications, d'interconnexions non prévues) ;
- des vulnérabilités ont été détectées et peuvent remettre en cause le niveau de sécurité du SI de manière inacceptable pour l'AH ;
- les menaces sur le SI ont significativement évolué ;
- des problèmes d'application des mesures de sécurité ont été identifiés, notamment lors d'un contrôle ou d'un audit ;
- le MCS du SI n'est pas applicable ou suffisamment appliqué, ou a été défaillant ;
- le système a fait l'objet d'un incident de sécurité significatif mettant en doute le niveau de sécurité attendu.

Le RSSI ou l'AE peut proposer à l'AH, *via* son centre expert, une suspension d'une décision d'homologation. Sur l'avis de son centre expert, l'AH peut réunir la commission d'homologation pour statuer sur la décision d'homologation.

Après suspension d'une décision, une démarche d'homologation sous réserve peut être réalisée avec un plan d'actions associé, ou le SI doit être mis hors service.

4.4. Abrogation d'une homologation

Une homologation est abrogée dès que le SI est retiré du service. Cette abrogation n'appelle pas de formalisme particulier mais doit être notifiée dans l'outil de suivi du patrimoine applicatif du ministère des Armées. L'AH est chargée de veiller à cette notification.

Le RSSI informe l'AH de l'abrogation de l'homologation.

4.5. Renouvellement des homologations

La démarche d'homologation pour renouveler une décision d'homologation est réalisée par :

- le RSSI-A si le SI est uniquement en phase d'utilisation ;
- le RSSI-P lorsque le SI est encore en phase de réalisation.

Selon l'importance des évolutions et de la criticité du SI, et sur proposition de son centre expert, l'AH peut renouveler la décision d'homologation sur simple présentation du dossier d'homologation réactualisé ou à partir de l'avis d'une nouvelle commission d'homologation.

Si le SI n'a pas connu de changements significatifs ou d'incidents majeurs ayant remis en cause ses besoins de sécurité, il n'est pas nécessaire de conduire à nouveau une démarche d'homologation complète.

- RO 27 :** il est **OBLIGATOIRE** qu'un renouvellement d'homologation comporte *a minima* :
- une revue des informations figurant dans le dossier d'homologation ;
 - une revue des informations d'enrôlement dans l'outil de suivi du patrimoine applicatif du ministère des Armées ;
 - une vérification des hypothèses de l'analyse de risques ;
 - une vérification de la pertinence des exigences de sécurité appliquées sur le SI ;
 - une revue du PTR ;
 - un bilan des contrôles SSI et audits réalisés sur le SI ;
 - un bilan de l'activité liée au MCS pour évaluer sa performance et identifier les événements marquants

Le renouvellement d'homologation peut donner lieu à un contrôle SSI ou à un nouvel audit.

La décision de renouvellement d'homologation est identique à celle d'une homologation et se présente de la même manière (cf. §4.2). Elle précise la référence de la précédente homologation.

5. CAS D'USAGE

5.1. Système d'information d'importance vitale

5.1.1. *Démarche d'homologation d'un SIIV*

RO 28 : il est **OBLIGATOIRE** de mener une démarche d'homologation de type standard pour homologuer un SI déclaré d'importance vitale. Toute dérogation à cette règle nécessite l'autorisation formelle du FSSI.

L'AH du SI est l'opérateur d'importance vitale (OIV), sauf cas particulier précisé dans la réglementation interministérielle ou ministérielle (cf. par exemple §5.11). S'il n'est pas l'AH du SI, il est membre de droit de la commission d'homologation. L'opérateur est identifié dans la stratégie d'homologation.

Le périmètre d'homologation définit les activités remises en cause en cas de dysfonctionnement ou d'atteinte à la sécurité numérique du SI, ainsi que les fonctionnalités qui les portent.

Les exigences de sécurité à appliquer, c'est-à-dire le socle de sécurité, contiennent nécessairement les règles définies par **[SIIV]**. Toute non-conformité à ces règles est dûment justifiée dans le dossier d'homologation.

La démarche d'homologation comprend nécessairement un audit dont les résultats et les actions qui en découlent sont étudiées lors de la commission d'homologation.

Des indicateurs de sécurité prévus par **[SIIV]** sont élaborés au cours de la démarche d'homologation et présentés à l'AH. Ils doivent permettre d'évaluer le niveau de sécurité du SI dont :

- le MCS du SI ;
- l'avancement de la démarche d'homologation ou de son renouvellement ;
- l'avancement du PTR mis en place.

Au-delà des documents correspondant à une démarche standard (cf. ANNEXE 1), le dossier d'homologation contient en outre :

- le formulaire de déclaration en SIIV, ainsi que les pièces le justifiant, dont l'analyse d'impacts ;
- la liste des indicateurs de sécurité et les modalités pour les déterminer.

5.1.2. **Décision d'homologation d'un SIIV**

En plus des éléments classiques à prendre en compte (cf. §4.1) pour statuer sur l'homologation du SI, l'AH doit aussi prendre en considération :

- la gestion des incidents ;
- la gestion de crise en cas d'attaques informatiques majeures ;
- les indicateurs de sécurité ;
- les rapports de sécurité prévus par le régime **[SIIV]**.

La durée de validité de l'homologation d'un SIIV non classifié est au maximum de 5 ans. En cas de SIIV classifié, elle dépend de son niveau de classification (cf. §4.3).

La décision et le dossier d'homologation sont à la disposition de l'agence nationale de la sécurité des systèmes d'information (ANSSI).

Il est rappelé que la décision d'homologation et le dossier d'homologation sont « des documents confidentiels susceptibles de contenir des informations dont la révélation est réprimée par les dispositions de l'article 226-13 du code pénal. Il est, le cas échéant, couvert par le secret de la défense nationale. » **[SIIV]**

La mention qu'un SI est SIIV est considérée a minima comme une information de niveau DIFFUSION RESTREINTE SPÉCIAL FRANCE.

RO 29 : il est **OBLIGATOIRE** de traiter et de protéger la décision d'homologation et le dossier d'homologation d'un SIIV **a minima** comme des documents de niveau de confidentialité DIFFUSION RESTREINTE et SPÉCIAL FRANCE. Selon les éléments qu'ils contiennent, ils peuvent être classifiés.

Il est possible d'émettre un extrait de décision d'homologation sans éléments protégés afin de faciliter sa diffusion.

La liste complète des SIIV d'un OIV est de niveau de classification SECRET et de mention SPÉCIAL FRANCE. Par conséquent, tout outil permettant de recenser les SIIV doit être de niveau de classification SECRET et de mention SPÉCIAL FRANCE.

RO 30 : il est **INTERDIT** d' enrôler les SIIV dans un outil non classifié si celui-ci mentionne sa catégorisation de SIIV..

5.2. Traitement de données classifiées

« Pour les systèmes d'information, la décision d'homologation du système vaut décision de classification. » [IGI 1300]

Le secrétariat général de la défense et de la sécurité nationale (SGDSN) est l'AH pour les SI traitant d'informations classifiées au niveau TRÈS SECRET faisant l'objet d'une classification spéciale ([IGI 1300]).

RO 31 : il est **OBLIGATOIRE** dans le cas de l'homologation d'un système traitant d'informations classifiées TRÈS SECRET faisant l'objet d'une classification spéciale de saisir formellement le haut fonctionnaire correspondant de défense et de sécurité (HFCDS) pour le lancement de toute démarche d'homologation, l'AH étant dans ce cas le SGDSN.

Dans le cadre d'un SI traitant des informations classifiées, la décision d'homologation atteste que les mesures nécessaires pour les protéger ont été mises en place et que le risque de compromission de ces informations a fait l'objet d'un traitement approprié afin de réduire, de manière acceptable, son niveau de vraisemblance [IGI 1300].

RO 32 : il est **OBLIGATOIRE** de mettre en destinataire des décisions d'homologation de SI classifiés, le FSSI et l'ANSSI.

Des dérogations à des exigences définies dans [IGI 1300] nécessitent des justifications formelles à insérer dans le dossier d'homologation. Pour les SI de niveau TRÈS SECRET, elles doivent être notifiées à l'ANSSI et au FSSI, et requièrent leur autorisation.

« Un dispositif de sécurité mis en place dans un SI qui traite d'informations classifiées est agréé par l'ANSSI lorsqu'il est utilisé, en complément de mesures organisationnelles de sécurité, comme un moyen essentiel de protection contre les accès non autorisés aux informations classifiées ou au système. » [IGI 1300] **Son usage doit alors respecter les conditions d'emploi et les exigences définies dans leur agrément.**

À titre exceptionnel et sur le fondement d'une analyse de risques complète, l'AH peut autoriser le recours à des matériels et logiciels agréés à un niveau inférieur, voire non agréés lorsqu'il n'existe pas de dispositif de sécurité agréé au bon niveau [IGI 1300].

RO 33 : il est **OBLIGATOIRE** de procéder à une démarche standard pour homologuer des SI classifiés dont les moyens essentiels de protection contre les accès non autorisés aux informations classifiées ou au système sont assurés par des matériels et logiciels agréés à un niveau inférieur exigé, voire non agréés lorsqu'il n'existe pas de dispositif de sécurité agréé au bon niveau. L'AH justifie l'autorisation de leur utilisation. La justification est insérée dans le dossier d'homologation.

Toutefois, sur proposition de son CEAH, une AH peut décider de déroger à la règle sous certaines conditions détaillées ci-dessous.

La règle ne s'applique pas pour une homologation d'un dispositif d'interconnexion ou d'un segment d'interface (cf. §5.11.1)

Conditions de dérogations à la règle RO33 :

Sur proposition de son CEAH, l'AH peut décider de déroger à la règle RO34 pour certains SI de niveau SECRET, et mener une démarche d'homologation simplifiée. Cette dérogation peut être mise en œuvre pour des SI isolés et simples [SI ISOLE], hors SI du contrôle gouvernemental et hors SIIV.

[SI ISOLE] « Un système d'information dit « isolé et simple » est le regroupement d'un ou de plusieurs ordinateurs fixes ou portables, éventuellement équipés de périphériques (d'affichage, de transfert de données ou de sauvegarde sur support de masse, de numérisation ou d'impression), isolé de tout réseau externe. Ce type de système intègre des équipements d'interconnexion (commutateurs) permettant la communication entre les ordinateurs. A noter qu'un système d'information hébergeant des annuaires d'administration (LDAP, Active Directory) ne rentre pas dans cette catégorie. Si une connexion réseau est possible entre plusieurs ordinateurs du même système d'information, celle-ci doit se faire exclusivement par le biais de réseaux filaires. Les réseaux sans fil ne doivent pas être utilisés dans ce type de système d'information. »

5.3. Traitement de données à caractère personnel

Le responsable de traitement (RT) a pour mission de déterminer les finalités et les moyens du traitement. Il assume la responsabilité juridique et supporte les sanctions en cas de non-respect des dispositions du RGPD.

L'homologation d'un SI traitant des données à caractère personnel relevant du périmètre du RT assure à ce dernier que les risques sur la sécurité des données à caractère personnel et leur protection au sein de ce SI ont été examinés et traités sur le plan technique conformément aux exigences réglementaires.

Elle doit donc nécessairement prendre en compte les risques suivants portant sur les personnes concernées :

- accès illégitimes à leurs données (confidentialité) ;
- modification non désirée de leurs données (intégrité) ;
- disparition de leurs données (disponibilité).

RO 34 : il est **OBLIGATOIRE** de préciser sur la décision d'homologation que le SI traite des données à caractère personnel lorsque ce traitement donne lieu à un acte réglementaire¹³.

¹³ Acte réglementaire portant création du traitement (arrêté publié aux journaux officiels).

Les traitements de données à caractère personnel qui font l'objet d'un acte réglementaire sont rappelés dans la **[FICHE 2 DCP]** publiée par la direction des affaires juridiques (DAJ). Ne sont pas soumis à la publication d'un acte réglementaire les traitements mis en œuvre aux fins de :

- gestion des comptes et accès informatiques, de la téléphonie fixe et mobile, des SI ;
- gestion des procédures d'achat (fichiers fournisseurs) et des fichiers clients ;
- gestion des opérations de communication (gratuites) ;
- gestion du courrier et des dossiers ;
- gestion des biens.
- La décision d'homologation d'un SI traitant des données à caractère personnel doit être transmise au(x) responsable(s) de traitement concerné(s).

Lors d'un traitement de données à caractère personnel relevant de son périmètre, le RT peut être amené à réaliser une analyse d'impact relative à la protection des données à caractère personnel (AIPD) sur les personnes concernées **[IM DAJ-RGPD]**. **L'AIPD n'est pas un prérequis à toute décision d'homologation.**

S'il est estimé nécessaire ou s'il est obligatoire de réaliser une AIPD, le RSSI contribue à l'élaboration de son volet technique au profit du RT. L'AH peut être amenée à se prononcer sur l'efficacité et la pertinence des mesures techniques mises en œuvre.

5.4. Homologation « sous réserves »

Dans les cas d'urgences politiques, stratégiques ou opérationnelles, l'autorité d'homologation peut prononcer une homologation sous réserves, décision qui correspond à une autorisation provisoire d'emploi (APE).

Pour des systèmes d'information ayant des risques résiduels trop importants mais devant être homologués pour des raisons stratégiques ou opérationnelles, **une décision d'homologation « sous réserves »** peut être proposée. Celle-ci permet d'autoriser l'emploi du système d'information et nécessite que les actions identifiées pour lever les réserves soient menées dans un délai de 12 mois maximum. La levée de réserves permet au système d'information de garder son homologation au-delà de la période définie **[GUIDE HOMOLOG]**.

RO 35 : il est **CONSEILLÉ**, dans des cas d'urgence stratégique ou opérationnelle, d'instruire une première décision d'homologation formelle, de préférence à une homologation sous réserves.

Une homologation « sous réserves » est limitée à une durée plus courte qu'une homologation formelle, le temps que la démarche soit finalisée. Elle est associée à un plan de mise en conformité.

Quelle que soit la démarche entreprise, l'homologation « sous réserves » nécessite *a minima* :

- une première stratégie d'homologation, comprenant obligatoirement le périmètre d'homologation, même succinct ;
- une analyse de conformité par rapport aux exigences essentielles définies par l'AH ;
- l'identification et l'évaluation des principaux risques résiduels qui pèsent sur le SI dans son contexte d'emploi ;
- la mise en place de procédures définissant la gestion des accès, des journaux et des incidents ;
- la définition et le suivi des actions nécessaires pour obtenir une première décision d'homologation.

L'AH doit s'assurer que la démarche d'homologation sera suivie jusqu'à son terme et aboutira à une décision d'homologation formelle avant la fin de validité de l'homologation « sous réserves ».

5.5. Déploiement opérationnel (OPEX, OPINT, exercice, etc.)

Par déploiement opérationnel, la présente directive entend les exercices, les missions ponctuelles ou les ouvertures de théâtre. Ils font l'objet d'une organisation SSI spécifique qui a la charge, entre autres, des déploiements de l'ensemble des SI de la mission. Il est donc possible de faire des homologations groupant tous les SI relevant de la responsabilité d'une même autorité, formellement définie dans le cadre de la mission.

Les PES applicables sur les SI déployés pour la mission peuvent être regroupées dans un seul document ou dans des CUC prédéfinis afin d'éviter d'inutiles redondances. Dans ce cas, l'AH décide d'une homologation de déploiement conformément à la procédure définie dans la présente directive (cf. §5.6) en faisant référence aux homologations de référence des SI déployés.

En cas de déploiement d'un nouveau SI au cours de l'opération, soit l'homologation de déploiement opérationnel doit être renouvelée pour intégrer ce SI, soit ce SI doit faire l'objet d'une homologation de déploiement spécifique.

5.6. Déploiements successifs d'un même SI

5.6.1. *Présentation*

Lorsqu'un SI de référence peut être déployé sur des instances, des sites ou dans des contextes d'emploi différents, la démarche d'homologation du SI à déployer peut s'appuyer sur une démarche d'homologation du SI de référence associée à des homologations de déploiement.

L'homologation du SI de référence est le préalable à toute autorisation d'exploitation en contexte d'emploi. La décision d'homologation du SI de référence est identique à celle d'une décision d'homologation classique et respecte les règles définies dans le présent document (cf. §4). Il est précisé que la durée de validité doit être cohérente avec l'évolutivité du contexte sécuritaire du SI.

L'homologation du SI à déployer dans son contexte d'emploi, appelée **homologation de déploiement**, est alors une déclinaison de l'homologation du SI de référence dans un contexte d'emploi et un environnement donnés. L'homologation de déploiement est alors la décision préalable à l'exploitation d'un SI de référence en contexte d'emploi.

Le dossier d'homologation du SI à déployer est constitué d'éléments génériques, stipulant les informations à compléter pour un déploiement dans le but de faciliter sa constitution et de limiter les efforts de rédaction.

5.6.2. *Procédure*

RO 36 : il est **OBLIGATOIRE** de préciser formellement dans la stratégie d'homologation du SI de référence la procédure de l'homologation de déploiement, ainsi que les différents responsables et les livrables attendus

L'AH du SI de référence est aussi l'AH du SI déployé ou délègue une partie de ses attributions à une autre autorité formellement désignée, notamment dans le cas d'un déploiement opérationnel (cf. §5.5).

Le RSSI du SI de référence conduit l'homologation du SI de référence et élabore la procédure d'homologation de déploiement. Celle-ci doit être adaptée aux contextes d'emploi, à l'environnement du déploiement, à sa pérennité et aux enjeux de sécurité.

Le responsable de la mise en œuvre de la procédure d'homologation de déploiement est défini par la stratégie d'homologation. Agissant sous la responsabilité de l'AE du SI déployé, il est en étroite relation avec le RSSI du SI de référence.

RO 37 : il est **OBLIGATOIRE** que le RSSI du SI de référence suive ses déploiements et leur état d'homologation. Il coordonne les différentes démarches d'homologation de déploiement.

Le CEAH vérifie la régularité de la procédure d'homologation définie dans la stratégie d'homologation.

Pour obtenir une homologation de déploiement, l'AE du SI et, si besoin, l'autorité en charge de l'exploitation technique du SI, doivent attester de la conformité au dossier d'homologation de référence au travers de CUC correspondant à leur domaine de responsabilité et, le cas échéant, du traitement des non-conformités.

Les éléments spécifiques du déploiement, ainsi que les modalités de traitement des non-conformités, sont formellement définis dans les PES locales, qui sont les déclinaisons locales des PES du SI de référence, ou encore dans un CUC selon le contexte de déploiement et les enjeux de sécurité.

La décision d'homologation de déploiement est identique à celle d'une décision d'homologation et se présente sous la même forme. Cependant, la décision d'homologation du SI de référence, sa date de fin de validité et sa référence doivent y être mentionnées.

La fin de validité d'une homologation de déploiement ne doit pas dépasser celle de l'homologation de référence.

5.6.3. Homologation de déploiement dérogatoire

L'homologation de déploiement étant une déclinaison de l'homologation de référence, cette dernière est un préalable obligatoire. Toutefois, **de manière exceptionnelle, lorsque le besoin opérationnel l'exige et si l'AH du SI déployé en accepte les risques**, une homologation de déploiement par l'AH peut être accordée sans attendre l'homologation complète du SI de référence. Elle est alors dite **dérogatoire**¹⁴.

Pour mettre en œuvre une homologation de déploiement dérogatoire (HDD), il est nécessaire de :

- désigner localement un RSSI en charge de la démarche d'homologation de déploiement ;
- mener une analyse de conformité au niveau technique et organisationnel à partir de CUC fournis par le RSSI du SI de référence ;
- présenter à l'AH du SI déployé les risques qui pèsent sur le SI.

La décision est limitée à une durée courte, le temps que la démarche d'homologation du SI de référence soit finalisée. La durée doit aussi rester cohérente avec la nature du SI considéré et la pérennité du déploiement. **La dérogation est conditionnée à la poursuite de l'instruction de l'homologation de référence.**

RO 38 : il est **OBLIGATOIRE**, pour une homologation de déploiement, y compris dérogatoire, que la décision d'homologation du SI déployé s'appuie sur des CUC et des PES locales.

L'HDD ne peut être renouvelée qu'une seule fois. Au-delà, si l'homologation de référence n'a toujours pas pu être prononcée, il convient de revoir la conception du SI qui est manifestement incompatible avec les objectifs de sécurité initialement validés.

¹⁴ La décision d'HDD est différente d'une APE. La HDD porte sur un SI déployé dont le SI de référence n'est pas encore homologué (cas du déploiement multiple d'un même SI) alors que l'APE porte sur un SI non homologué à déployer.

Le RSSI du SI de référence est informé de la décision et informe l'AH du SI déployé.

RO 39 : il est **INTERDIT** de renouveler plus d'une fois une HDD.

5.6.4. Renouvellement de l'homologation

5.6.4.1. Renouvellement de l'homologation du SI de référence

Les conditions de renouvellement d'homologation du SI de référence sont identiques à celles d'une homologation classique. Elles sont définies par la stratégie d'homologation.

À la procédure définie dans [§5.6], s'ajoutent :

- un point de situation des SI déployés et de leur état d'homologation ;
- un contrôle des procédures mises en œuvre pour homologuer les SI déployés et pour garantir leur MCS.

Lors de la commission d'homologation, il est décidé de renouveler ou non les décisions d'homologation des SI déployés.

5.6.4.2. Renouvellement de l'homologation du SI déployé

Les conditions de renouvellement sont définies dans la stratégie d'homologation du SI de référence.

Une décision d'homologation de déploiement doit être renouvelée lorsque :

- elle est arrivée en fin de validité ;
- l'AH du SI de référence le demande ;
- les conditions du déploiement ont changé de manière substantielle.

Le renouvellement d'homologation du SI déployé doit comporter *a minima* :

- un contrôle de conformité du SI à l'homologation de référence au travers des CUC réactualisés par le RSSI du SI de référence ;
- un contrôle de la configuration du SI ;
- un contrôle de qualification des exploitants¹⁵ ;
- une revue et une mise à jour des procédures de sécurité.

Le RSSI du SI de référence est informé des résultats des contrôles, ainsi que des modifications de procédures de sécurité.

RO 40 : il est **OBLIGATOIRE**, lors d'un renouvellement d'homologation du SI de référence, de procéder au renouvellement des homologations de déploiements liées à la précédente décision d'homologation

5.6.5. Suspension et abrogation de l'homologation de déploiement

Les cas de suspension et d'abrogation de la décision d'homologation de déploiement sont identiques à ceux d'une homologation classique (cf. § 5.4 et 5.5).

En cas de suspension ou d'abrogation de l'homologation du SI de référence, la décision d'homologation des SI déployés est de fait suspendue ou abrogée.

¹⁵ Il s'agit de contrôler que le SI est toujours administré par un administrateur qualifié.

5.7. Homologation de SI similaires

Des SI différents peuvent être constitués de composants et d'une architecture similaires, déployés dans un même environnement, ayant les principaux besoins de sécurité identiques et relevant d'une même AQSSI. Leur homologation peut alors être facilitée.

Les points suivants doivent être similaires entre le système d'information de référence et le SI similaire :

- classification des données hébergées et du système d'information ;
- type de localisation (local sécurisé, conditions d'accès, ...) ;
- plan de maintien en condition de sécurité ;
- modèle d'administration ;
- profil des utilisateurs ;
- autorité d'homologation.

À chaque homologation de SI similaires, le dossier d'homologation pourra s'appuyer sur le dossier d'homologation du SI de référence.

À partir de l'homologation d'un premier SI, dit de référence, il est donc possible d'homologuer un SI qui lui est similaire en réalisant **une analyse de conformité par rapport à un CUC spécifique**.

Le CUC est établi par le RSSI, validé par l'AH et permet de définir les exigences de sécurité à respecter pour être homologué. La stratégie d'homologation du SI similaire détermine la pertinence d'ajuster la durée d'homologation en fonction de celle du SI de référence.

5.8. Homologation de SI hébergés au ministère

Le niveau de sécurité numérique du SI hébergé dépend de celui du SI hébergeur et du niveau de sécurité que celui-ci apporte au SI hébergé. La démarche d'homologation d'un SI hébergé dans un système relevant du ministère doit prendre en compte *a minima* :

- les services de sécurité proposés par le SI hébergeur ;
- les conditions d'utilisation du SI hébergeur, et particulièrement les exigences de sécurité qu'il impose au SI hébergé, par exemple sous la forme d'un CUC fourni par l'opérateur en charge du SI hébergeur ;
- les objectifs de sécurité du SI hébergeur, définis dans sa politique de sécurité ;
- l'homologation du SI hébergeur et ses conditions de validité.

La décision d'homologation du SI hébergeur et ses conditions d'utilisation, notamment les exigences de sécurité qu'il impose au SI hébergé, et ses objectifs de sécurité doivent être connus du RSSI du SI hébergé et insérés dans le dossier d'homologation.

La décision d'homologation du SI hébergeur demeure valide si les SI qu'il héberge ne remettent pas en cause ses conditions de validité ou son niveau de sécurité.

La décision d'homologation du SI hébergé peut être remise en cause par :

- la suspension de la décision d'homologation du SI hébergeur ;
- un changement conséquent dans le SI hébergeur et les services qu'il fournit au SI hébergé ;
- un incident majeur survenant sur le SI hébergeur.

RO 41 : il est **OBLIGATOIRE**, lors d'un renouvellement d'homologation du SI de référence, de procéder au renouvellement des homologations de déploiements liées à la précédente décision d'homologation

5.9. Homologation de SI utilisant un service d'informatique en nuage externalisé

L'homologation dépend du niveau de maîtrise dont dispose le ministère des Armées à l'égard des solutions proposées par le prestataire de service d'informatique en nuage.

RO 42 : il est **OBLIGATOIRE** d'homologuer les systèmes ou services numériques fournis par un prestataire de services d'informatique en nuage pour traiter des données relevant du ministère des Armées selon un périmètre d'homologation défini en fonction de la nature du service rendu ou du produit fourni.

RO 43 : il est **OBLIGATOIRE** de demander au prestataire d'informatique en nuage externalisé de fournir un PAS (plan d'assurance de sécurité). Le PAS produit par le prestataire est alors inséré dans le dossier d'homologation.

5.9.1. Solution publique de type IaaS ou PaaS

La solution dans sa totalité ne peut pas faire l'objet d'une décision d'homologation. Le périmètre d'homologation doit en effet s'appuyer sur **une distinction précise des responsabilités** relevant du ministère et du fournisseur de service. Les composants relevant du seul prestataire n'entrent pas dans le périmètre d'homologation, même si la démarche d'homologation les prend nécessairement en compte dans l'analyse de risques. Il ne s'agit pas d'homologuer le SI du prestataire.

RO 44 : il est **OBLIGATOIRE** de considérer dans le périmètre d'homologation l'utilisation et le cadre d'utilisation du service IaaS ou PaaS, tant dans sa dimension fonctionnelle que sécuritaire.

Les garanties et les éléments de confiance que peut produire le prestataire de service d'informatique en nuage participent à l'appréciation du risque. Ils doivent être recherchés et analysés. Les difficultés d'obtention et l'absence d'informations de la part des prestataires sont également des éléments de confiance à prendre en compte dans l'analyse.

5.9.2. Solution publique de type SaaS

L'utilisation d'un service numérique public de type SaaS nécessite au préalable :

- une appréciation d'usage du service numérique validée par l'AE ;
- un visa du CND conformément à **[CLOUD SaaS]** ;
- une décision d'homologation portant sur l'usage du service numérique.

L'appréciation d'usage est un document formel qui identifie et évalue les risques portant sur l'usage des services et sur les données traitées en termes juridique et de sécurité numérique. Elle est validée par l'AE et transmise à l'AH. L'AE peut s'appuyer sur le CEAH et sur le représentant du RT concerné (lorsque des données à caractère personnel y sont traitées).

L'analyse de risques, ainsi que la décision d'homologation, doivent s'appuyer sur l'appréciation d'usage du service numérique. L'appréciation d'usage est insérée dans le dossier d'homologation.

RO 45 : il est **OBLIGATOIRE** pour l'AE de fournir une appréciation d'usage à l'AH avant d'initier la démarche d'homologation portant sur l'usage du service numérique

Le périmètre d'homologation ne comprend que les données traitées et relevant du ministère des Armées, les services numériques fournis par le prestataire, ainsi que l'organisation mise en place pour utiliser ce service.

RO 46 : il est **OBLIGATOIRE** pour l'AE d'établir une politique d'emploi pour pouvoir utiliser un service numérique public de type SaaS. Elle est fournie à l'AH pour insertion dans le dossier d'homologation.

La **politique d'emploi** dédiée à l'usage du service numérique précise :

- les conditions générales d'utilisation du service numérique avec les mesures de sécurité associées relevant du ministère, ainsi que les responsabilités correspondantes ;
- les dispositions relatives à la gestion de données à caractère personnel utiles aux utilisateurs du service numérique ;
- la gestion des accès et leur contrôle ;
- les modalités de gestion des incidents et des crises ;
- les modalités de réversibilité et les mesures prises sur les données (transfert, effacement et archivage) lors de la fin de prestation.

Il appartient à l'AH de définir le besoin de rédiger des PES selon les exigences de sécurité complétant la politique d'emploi.

Lorsque le service numérique traite des données à caractère personnel, la politique de confidentialité du prestataire est insérée dans le dossier d'homologation. Elle est prise en compte dans l'analyse de risques.

5.10. Homologation de systèmes de systèmes

Un système complexe peut être composé de plusieurs SI interdépendants techniquement, formant ainsi un système de systèmes, dont l'homologation est à traiter de manière spécifique. En effet, il est possible, selon les cas, d'homologuer ce système en homologuant successivement ou parallèlement ses différents composants.

Néanmoins, des risques peuvent être identifiés et acceptés pour chacun de ses composants sans que cela signifie nécessairement que l'ensemble des risques soient identifiés et acceptables au niveau du système. De même, un système de systèmes ne perd pas nécessairement son homologation quand l'un de ses composants n'est plus homologué. **L'homologation d'un système de systèmes ne se réduit donc pas à une succession d'homologations séparées.** Elle doit aussi prendre en compte les risques portant sur les interdépendances techniques et sur l'ensemble du système.

RO 47 : il est **RECOMMANDÉ** pour une homologation d'un système de systèmes de procéder à une analyse de risques portant non seulement sur chacun de ses composants mais également sur l'ensemble du système de systèmes et l'interdépendance de ces derniers.

L'homologation d'un système de systèmes est mise en œuvre par un RSSI. Celui-ci coordonne les homologations des différents composants et s'assure de la gestion de risques d'ensemble.

La stratégie d'homologation doit préciser les conditions de l'homologation et les principes de sa cohérence d'ensemble en matière de sécurité numérique.

5.11. Dispositifs d'interconnexion ou d'interface

Pour toute interconnexion de SI de niveaux de classification différents ou entre un SI classifié et un SI non-classifié, interdite en principe, il est nécessaire que l'AE la justifie formellement auprès de l'AH et de l'AQSSI par un besoin opérationnel [IGI 1300]. La justification formelle est insérée dans le dossier d'homologation.

RO 48 : il est **OBLIGATOIRE** pour toute interconnexion de SI de niveaux de classification différents, ou entre un SI classifié et un SI non-classifié, de la justifier formellement par l'AE auprès de l'AH et de l'AQSSI par un besoin opérationnel.

5.11.1. Homologation spécifique

RO 49 : il est **OBLIGATOIRE** de procéder à une homologation **spécifique** des interconnexions ou de segments d'interface de SI de même niveau de classification. L'interconnexion ou le segment d'interface de SI est alors homologué au même niveau de classification que ces systèmes

RO 50 : il est **OBLIGATOIRE** de procéder à une homologation **spécifique** des dispositifs d'interconnexion ou des segments d'interface de SI de niveaux de sensibilité ou de classification différents, ou de SI externes au ministère des Armées. L'interconnexion ou le segment d'interface de SI est alors homologué au niveau du SI le plus élevé.

L'interconnexion ou les segments d'interface font l'objet d'une homologation distincte de celles des réseaux [II 901].

RO 51 : il est **RECOMMANDÉ** de procéder à une homologation **spécifique** des dispositifs d'interconnexion ou des segments d'interface de SI non classifiés et relevant tous du ministère des Armées.

5.11.2. Désignation de l'autorité d'homologation

L'AH d'une interconnexion ou d'un segment d'interface est :

- de manière générale, l'AH désignée après concertation entre les AH de chaque SI interconnecté ;
- par défaut, l'AH du SI du niveau de classification le plus élevé dans le cas de SI de niveaux de classification différents ;
- le SGDSN ou toute autorité à qui il en délègue la responsabilité, dans les cas suivants [IGI 1300] :
 - o pour les transferts d'informations entre des SI classifiés de même niveau, dont l'un n'est pas sous maîtrise nationale ;
 - o pour les transferts d'informations entre des SI classifiés de même niveau, dont l'un est amené à traiter des informations classifiées de l'Union européenne ou de l'OTAN ;
 - o lorsque l'utilisation de dispositifs de sécurité agréés est obligatoire mais impossible, notamment lorsqu'il n'existe pas de dispositif de sécurité agréé ou lorsqu'il n'est pas agréé au bon niveau.

5.12. Capacités opérationnelles (interdépendances fonctionnelles)

Une capacité opérationnelle est un ensemble de SI qui concourent à la réalisation d'une fonction métier ou qui constituent un écosystème d'un ensemble opérationnel.

L'homologation d'une capacité opérationnelle permet aux AE de prioriser les efforts de sécurisation en fonction des priorités opérationnelles et du niveau de criticité des éléments composant cette capacité. Elle renseigne également sur le niveau de résilience de la capacité opérationnelle.

L'homologation d'une capacité opérationnelle nécessite au préalable une cartographie complète des interdépendances techniques et fonctionnelles entre les différents éléments concourant à cette capacité.

5.13. Homologation d'un SI développé en mode agile

5.13.1. Homologation itérative

Le mode de développement en agilité se caractérise par un développement itératif du SI et par sa mise en exploitation alors qu'il est encore en phase de réalisation. À chaque cycle de développement (« *build* »), de nouvelles fonctionnalités sont créées, faisant ainsi évoluer le SI en production.

Le choix de l'agilité ne réduit pas les risques en matière de sécurité numérique qui dépendent de la sensibilité du SI et des probabilités d'une cyberattaque à son encontre. La méthode d'analyse de risques n'est donc pas modifiée du fait de l'agilité du projet.

Dans ce cas, la démarche d'homologation est elle-même itérative. Elle doit aboutir au moins à deux décisions d'homologation :

- **une décision d'homologation initiale** permettant de mettre en exploitation le SI après le premier incrément ;
- **une décision d'homologation ferme**, une fois le développement terminé, pour le transfert définitif de l'exploitation à l'opérateur et conduisant au démantèlement de l'équipe de développement.

Eventuellement, si l'évolution en cours de développement le nécessite, la décision d'homologation initiale peut être renouvelée avant d'atteindre une décision ferme. La décision d'homologation est alors dite **transitoire**.



Figure 1. Processus d'homologation d'un SI développé en mode agile

Une décision d'homologation initiale doit être prononcée avant une première mise en exploitation du SI.

La durée de validité des décisions d'homologation (initiale, transitoire, ferme) est à la diligence de l'AH dans les limites réglementaires (cf. §4.3) et en fonction du niveau de contrôle qu'elle estime nécessaire.

La démarche d'homologation impose **la mise en place de relations entre les équipes de projet et le CEAH**. Ces relations se formalisent au moins par des compte-rendus continus des travaux relatifs à la sécurité que l'équipe de projet adresse au CEAH. Pour faciliter les échanges entre le RSSI et l'équipe de développement, et selon la dimension de cette dernière, il est possible de désigner parmi les membres de l'équipe de développement un référent en matière de sécurité numérique.

La démarche d'homologation mise en œuvre est identique à celle d'une démarche sommaire, simplifiée ou standard.

Les pièces du dossier d'homologation évolueront au fur et à mesure du développement.

5.13.2. Décision d'homologation initiale

La décision d'homologation initiale a pour but de valider :

- le niveau de sécurité du premier incrément du SI ;
- le processus itératif mis en œuvre pour les incréments suivants. Couvrant la conception jusqu'à la mise en exploitation, il doit viser à intégrer la sécurité au fil de l'eau ;
- le processus pour le MCS du SI.

RO 52 : il est **OBLIGATOIRE** de mentionner dans la stratégie d'homologation les modalités des échanges entre les différents acteurs (RSSI, équipe de développement, CEAH), le rythme des remontées d'informations, ainsi que les conditions de maintien de l'homologation.

L'homologation initiale décrit les fonctionnalités envisagées pour le SI (« *user stories* »).

L'analyse de risques mise en œuvre a pour objectif d'identifier et d'évaluer les risques de sources intentionnelles (« *evil user stories* ») et non intentionnelles (« *abuser stories* »). Elle donne lieu à une liste de risques résiduels portant sur le SI, liste à mettre à jour après chaque cycle de développement.

Dès la première mise en exploitation du SI, le RSSI rédige une première version de PES. Celles-ci doivent décrire l'organisation et les procédures de sécurité à appliquer durant l'exploitation.

5.13.3. Au cours du développement

Le RSSI met à jour systématiquement, après chaque cycle de développement, le périmètre d'homologation, ainsi que la liste des risques résiduels portant sur le SI. Le CEAH est informé des modifications apportées.

Pour chaque nouvelle fonctionnalité envisagée (« *user stories* »), des scénarios de risques (« *abuser stories* », « *evil user stories* ») doivent être étudiés et peuvent donner lieu à de nouvelles mesures de traitement des risques. Ces dernières doivent être priorisées et implémentées au même titre que les nouvelles fonctionnalités. Il est très fortement déconseillé de les accumuler dans le tableau de suivi des actions en ligne (« *back log* ») dans le but de consacrer les dernières itérations (« *builds* ») à la sécurité. Une telle démarche pourrait remettre en cause l'ensemble du développement.

Les PES sont mises à jour au fur et à mesure des itérations pour prendre en compte les nouvelles fonctionnalités implémentées.

Durant la phase de réalisation, la décision d'homologation initiale est remise en cause :

- systématiquement à la fin de la date de validité de la décision d'homologation précédente ;
- par l'AH sur proposition de son centre expert si les conditions décrites dans la décision d'homologation ne sont plus respectées ou si le traitement des risques n'est pas suffisamment pris en compte lors du développement :
 - soit en raison de l'évolution du SI :
 - fonctionnalités qui sortent du cadre initialement défini ;
 - changement important d'architecture ;
 - utilisation de nouvelles sources de données représentant un risque non anticipé ;
 - liste des fonctions SSI attendues (« *back log* ») augmentant de manière démesurée par rapport au reste des fonctionnalités ;

- soit en raison d'un dysfonctionnement dans les échanges d'informations entre les différents acteurs, tel le défaut de compte-rendus de la part de l'équipe de projet au profit du CEAH.

Lorsque la décision d'homologation est remise en cause, le RSSI procède à son renouvellement selon les modalités requises par le CEAH.

5.13.4. Décision d'homologation ferme

Une fois le développement terminé, une décision d'homologation ferme doit être prononcée. Elle garantit :

- la mise en œuvre du MCS ;
- la formation pérenne des administrateurs ;
- l'applicabilité et l'exhaustivité des contrats de service ;
- l'enrôlement du SI ;
- la bonne diffusion et l'applicabilité des PES.

La décision d'homologation ferme peut également s'appuyer sur un rapport d'audit final comme toute décision d'homologation.

5.14. Cas de mise en exploitation pour test ou expérimentation

Dans le cadre d'un développement ou d'une expérimentation, un SI peut nécessiter une mise en exploitation sur des réseaux opérationnels et peut éventuellement consommer des données réelles, notamment s'il n'est pas possible de créer des jeux de données fictives. Il est donc nécessaire de se prémunir des risques que ferait porter ce SI sur son environnement et sur les données qui lui sont confiées.

L'autorisation d'exploitation pour tests ou expérimentation¹⁶ est délivrée par l'AH sur étude du dossier d'homologation en cours de constitution qui devra couvrir les risques systémiques - notamment les risques à l'égard des SI interconnectés - et la confidentialité des données lorsque des données réelles sont utilisées. Une attention est également à porter sur le besoin de traçabilité.

Lorsque l'autorisation concerne un projet contenant des données à caractère personnel, il est obligatoire de demander l'autorisation d'utilisation de ces données à l'AH. Celle-ci pourra, selon le contexte, répondre favorablement ou non. La stratégie d'homologation définit les modalités d'une autorisation d'exploitation pour tests.

Les conditions du test et de sécurité doivent être définies dans un document formel (PES, plan de test et de sécurité, etc.) dans lequel seront notamment précisés :

- les responsabilités des acteurs en matière de sécurité ;
- les flux ouverts et leur gestion ;
- les SI et équipements interconnectés ;
- les mesures de sécurité à appliquer ;
- le devenir des données collectées et produites au cours du test.

¹⁶ Autorisation connue sous le nom d'AFT (*Approval for testing*).

RO 53 : il est **OBLIGATOIRE** que la mise en exploitation d'un SI pour test ou expérimentation soit subordonnée à l'autorisation formelle de l'AH qui valide les conditions de sécurité préalablement définies. Dans le cadre d'un test, la stratégie d'homologation doit prévoir cette autorisation et en préciser les modalités. L'autorisation d'exploitation est associée à une date de fin de validité et à un niveau de confidentialité des données à traiter.

5.15. Cas de régularisation

Si un SI en phase d'utilisation n'a pas fait l'objet d'une décision d'homologation, l'AH doit procéder à une démarche d'homologation pour régulariser la situation selon l'un des trois types de démarches (cf. §3.4.5).

Cependant, cette démarche peut être **progressive et aménagée** au regard des ressources allouées, de l'état du SI et de sa catégorisation, dans le cadre d'un processus d'amélioration continue. Elle nécessite au préalable une stratégie d'homologation et des PES qui pourront évoluer par la suite.

5.15.1. *Dossier d'homologation*

Quel que soit le type de démarche choisi, le dossier d'homologation peut être constitué des éléments suivants :

- une stratégie d'homologation précisant :
 - o les besoins de sécurité ;
 - o les modalités pour parvenir à une décision d'homologation ferme et entière ;
 - o les pièces du dossier d'homologation pour obtenir une première décision d'homologation ;
 - un périmètre d'homologation présentant :
 - o les principales données métier ;
 - o les équipements sensibles et leur localisation ;
 - o les interconnexions ;
 - des PES définissant :
 - o la gestion des accès ;
 - o la protection contre les codes malveillants ;
 - o la gestion des journaux ;
 - o le MCS ;
 - o la gestion des incidents ;
 - un PTR qui évoluera au gré du processus ;
 - une liste de non-conformités aux textes **[PMSN-S]** et **[PSSIM-T]**, auxquels s'ajoute **[IGI 1300]** en cas de SI classifié.
- Le SI est nécessairement enrôlé dans l'outil de suivi du patrimoine applicatif du ministère (cf. RO 8).
- En fonction du SI et de sa criticité, l'AH peut rajouter d'autres éléments à la liste ci-dessus.

Le dossier d'homologation et les pièces le constituant sont enrichis progressivement après la première décision d'homologation selon les modalités définies dans la stratégie d'homologation.

5.15.2. *Démarche d'homologation*

En cas de démarche sommaire, la procédure est à suivre sans aucun allègement (cf. §3.5.1).

En cas de démarche simplifiée, l'analyse de risques est réduite à une analyse de conformité aux textes **[PMSN-S]** et **[PSSIM-T]**, auxquels s'ajoute **[IGI 1300]** en cas de SI classifié. Cette analyse peut être menée au travers d'un contrôle interne portant sur le SI par le CEAH ou par une entité mandatée par l'AH. A partir de l'analyse, voire du contrôle, les risques sont identifiés et évalués. Le rapport de contrôle, ainsi que le plan d'actions qui en résulte, seront assimilés respectivement à la liste de non-conformités et au **PTR**.

En cas de démarche standard, l'analyse définie précédemment peut être conduite. Cependant, le contrôle est mené par une entité mandatée par l'AH, différente du CEAH. Les éléments définis comme particulièrement sensibles par l'AH, de nature technique ou organisationnelle, devront faire l'objet d'une analyse de conformité plus poussée en s'appuyant en particulier sur les directives du **CND** et les guides de recommandation de l'ANSSI.

5.15.3. Décision d'homologation

Pour apporter un avis à l'AH, la commission d'homologation doit s'assurer de :

- l'identification des principaux manquements aux textes **[PMSN-S]** et **[IGI 1300]** en cas de SI classifié, et aux autres textes en cas de démarche standard ;
- l'évaluation des risques que génèrent les manquements constatés ;
- l'acceptabilité de ces risques au regard des enjeux opérationnels et des ressources disponibles ;
- la faisabilité de mener une démarche d'homologation complète au regard des modalités prévues pour y parvenir, des ressources allouées, de l'état du SI et de sa criticité.
- Le temps de validité de la décision d'homologation pour régularisation doit permettre de finaliser la démarche, en particulier de mettre en place une analyse de risques complète en cas de démarche standard. Elle ne doit pas dépasser :
 - 1 an pour un SI essentiel ;
 - 2 ans pour un SI important ou standard.

ANNEXE 1. LE DOSSIER D'HOMOLOGATION

Le dossier d'homologation est un ensemble de documents sur lesquels s'appuie l'AH pour émettre un avis de décision d'homologation ou de renouvellement d'homologation. Il est réactualisé au fur et à mesure des démarches. Sa composition varie en fonction du type de démarche d'homologation, de la nature des SI et de ses composants et des enjeux de sécurité.

Livrables les plus usuels selon le type de démarche :

	Démarche sommaire	Démarche simplifiée	Démarche standard
Décision d'homologation	oui	oui	oui
Stratégie d'homologation	oui	oui	oui
Plan d'assurance de sécurité (PAS)	en cas d'infogérance externalisée (dont <i>cloud</i>)		
Certificat d'usage et de conformité (CUC)	oui	oui	
Dossier d'analyse de risques	non	oui	oui
Cible de sécurité	non	non	facultatif
Plan de sécurité (PDS)	non	non	oui
Procédures d'exploitation de sécurité (PES)	oui	oui	oui
Dérogations obtenues	oui	oui	oui
Rapport d'audit (conformité, code, etc.)	non	si audit réalisé	oui
Plan d'actions suite à un audit	non	si audit réalisé	oui
Liste des risques résiduels	oui	oui	oui
Plan de traitement des risques (PTR)	oui	oui	oui

Tableau 2. Livrables requis selon la démarche d'homologation

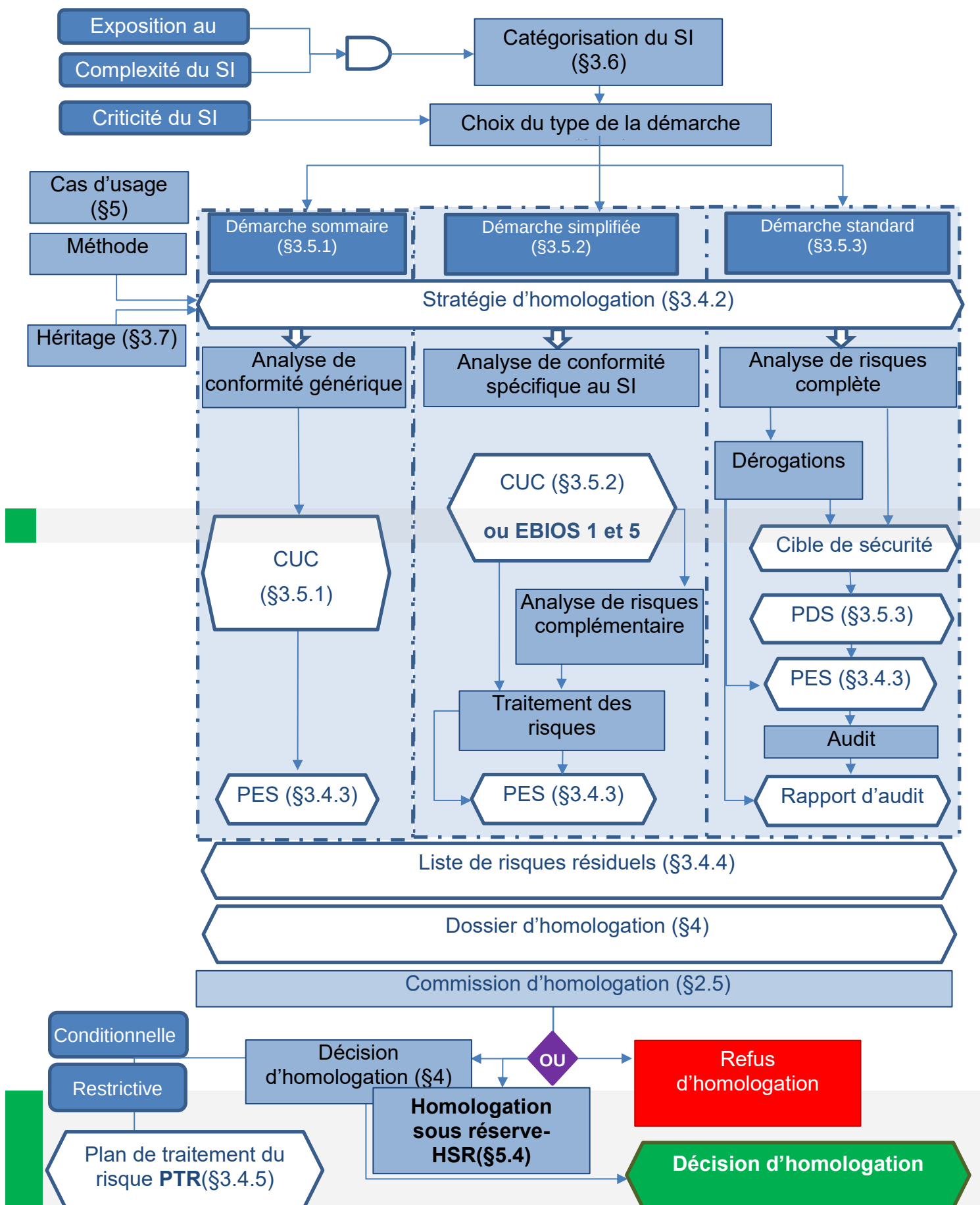
Les documents dont les noms sont en gras doivent être insérés dans l'outil de suivi du patrimoine applicatif (SICLADE).

Livrables supplémentaires possibles (liste non exhaustive) : le dossier d'homologation peut être enrichi d'autres documents, en particulier :

- en cas de démarche d'homologation de déploiement :
 - o les modèles nécessaires à l'homologation des SI déployés (CUC, PES, etc.) pour le dossier d'homologation du SI de référence ;
- en cas de SIIV :
 - o la déclaration en SIIV ;
 - o des pièces justificatives (analyse d'impact) ;
 - o des indicateurs de sécurité (cf. §5.1) ;
- en cas d'infogérance externalisée (par exemple *cloud*) :
 - o le PAS ;
- en cas de *cloud* SaS :
 - o le visa du CND ;
 - o une appréciation d'usage du service numérique ;

- en cas de SI traitant des données classifiées :
 - le rapport de mesures des signaux parasites compromettants ;
 - l'attestation de circuit approuvé ;
 - les justifications des non-conformité à l'égard de l'[IGI 1300] ;
- en cas d'utilisation de solutions de chiffrement :
 - les dossiers cryptographiques correspondants, validés par le HFCDS ou l'AQ SSI ;
 - l'ordre pour le chiffre ;
- en cas d'utilisation de produits de sécurité certifiés par l'ANSSI :
 - les certificats de sécurité de l'ANSSI, agréments de produits de sécurité ;
- en cas d'homologation de SI hébergé, la décision d'homologation du SI hébergeur ;
- en cas de besoin de forte résilience :
 - le plan de continuité/reprise informatique (PCI/PRI) ;
 - le PCA/PRA ;
- en cas de supervision de sécurité par un SOC :
 - tout document attestant de la capacité de mettre sous supervision le SI par un SOC (exemple : compte-rendu de faisabilité).

ANNEXE 2. SCHÉMA DE PRINCIPE DE L'HOMOLOGATION



ANNEXE 3. FORMATION : SAVOIR ET SAVOIR-FAIRE

DÉMARCHE D'HOMOLOGATION (CENTRE EXPERT DE L'AH)

Sensibilisation	
Déroutement d'un projet, d'un programme.	
Connaissances	
Organisation de la sécurité numérique du ministère, des EMDS	Rôle et responsabilité de l'AH et des RSSI dans une démarche d'homologation.
Directives relatives à l'homologation (27) et au MCS (47), Guide n°7.	Textes réglementaires interministériels et ministériels portant sur la sécurité du numérique.
Différents principes de la sécurité numérique (cf. Introduction Guide n°7).	Quelques notions sur les normes et standards (ISO 27000, NIST, guide ANSSI).
Différentes catégories de risques portant sur un système numérique (incident, attaque informatique) et leur réalité.	Quelques notions sur les types de technologie et les risques associés.
Notions essentielles d'une analyse de risques (besoin de sécurité, risques, menaces, vulnérabilités, impacts, risque résiduel, etc.)	Méthodes d'analyse de risques en usage au ministère
Principaux sites d'information (ANSSI, CERT-Fr, INTRADEF, CALID, etc.)	Aspects juridiques (SI, information)
Savoir-faire	
Identifier les différents acteurs d'une démarche d'homologation, d'un projet/programme	
Déterminer un référentiel réglementaire à partir de la nature du SI, des données et de ses principales fonctionnalités	
Élaborer et étudier un certificat d'usage et de conformité	
Mener une méthode d'analyse de risques ([EBIOS RM])	
Catégoriser un système numérique	

Mener une démarche d'homologation (sommaire, simplifiée, standard)
Étudier un dossier d'homologation et les pièces le constituant
Rédiger une synthèse d'une analyse portée sur une démarche et un dossier d'homologation
Présenter un risque à une autorité
Présenter une démarche d'homologation
Conseiller un RSSI sur la démarche d'homologation
Veiller sur l'actualité des risques, attaques et incidents portant sur les systèmes numériques

ANNEXE 4. LISTES DES EXIGENCES

N°	Statut (cf. §0)	Intitulé de la règle	Acteur ¹⁷
RO 1 :	Obligatoire	Pour tout SI du ministère, désigner formellement une AH pour un périmètre d'homologation donné.	AQSSI
RO 2 :	Recommandé	Désigner une AH pour tout SI au sein de la chaîne d'emploi du SI.	AQSSI
RO 3 :	Obligatoire	En cas de changement d'AH au cours du cycle de vie du SI, procéder formellement à un transfert de responsabilités au cours duquel le dossier d'homologation du SI est transmis à la nouvelle AH.	AQSSI
RO 4 :	Obligatoire	Renouveler la décision d'homologation en cas de transfert de responsabilité d'AH. La mise en œuvre de ce renouvellement est laissée à l'appréciation de l'AH prenante dans un délai maximal d'un an .	AH (prenante)
Erreur ! Source du renvoi introuvable.	Obligatoire	Pour une AH, disposer d'au moins un spécialiste SSI formé à la démarche d'homologation.	AH
RO 6 :	Obligatoire	Pour l'AH, constituer une commission d'homologation, adaptée au système à homologuer et en fixer les règles générales de fonctionnement.	AH
RO 7 :	Obligatoire	Dans le cadre d'une démarche d'homologation standard, constituer la commission d'homologation au minimum des acteurs suivants : - l'AH ou son représentant ; - le responsable SSI (RSSI) en charge de la démarche d'homologation ; - le responsable de projet (RCP ou équivalent)/programme ou son représentant ; - l'AE ou son représentant.	AH RSSI
RO 8 :	Obligatoire	Renseigner les informations relatives à la démarche d'homologation dans l'outil de suivi du patrimoine applicatif du ministère des Armées et les réactualiser au fur et à mesure de la démarche d'homologation (sous réserve du niveau de classification de ces informations).	AE RSSI
RO 9 :	Obligatoire	Afin que la décision d'homologation soit motivée et justifiée, pour l'AH, s'appuyer sur un dossier d'homologation conforme à la démarche d'homologation choisie et dont les pièces constitutives sont définies par la stratégie d'homologation.	AH
RO 10 :	Obligatoire	Pour le RSSI, constituer le dossier d'homologation tel qu'il est défini dans la stratégie d'homologation et le faire valider par le CEAH.	RSSI
RO 11 :	Obligatoire	Pour le RSSI, documenter le périmètre d'homologation, validé par l'AH, et l'actualiser au fur et à mesure de l'évolution du SI.	RSSI
RO 12 :	Obligatoire	Pour le RSSI, établir une stratégie d'homologation puis la faire approuver par l'AH.	RSSI
RO 13 :	Obligatoire	Pour le RSSI, rédiger des PES puis les faire approuver par l'AH, après accord de l'AE.	RSSI
RO 14 :	Obligatoire	Pour l'AH, délivrer une décision d'homologation à partir d'une liste de risques résiduels après avoir autorisé les mesures dérogatoires relevant de son périmètre.	AE AH

¹⁷ AQSSI autorité qualifiée en matière de SSI, AE autorité d'emploi, AH autorité d'homologation, RSSI responsable SSI (RSSI-A ou P)

N°	Statut (cf. §0)	Intitulé de la règle	Acteur ¹⁷
RO 15 :	Obligatoire	Pour l'AH, valider un plan de traitement du risque (PTR), celui-ci est initié et mis à jour par le RSSI dès la phase de développement du SI et tout au long du cycle de vie.	AH RSSI
RO 16 :	Obligatoire	Pour homologuer un SI, appliquer l'une des trois démarches d'homologation identifiées : sommaire, simplifiée ou standard.	AH RSSI
RO 17 :	Obligatoire	Pour l'AH, dans une démarche sommaire, fournir au RSSI le CUC qu'il devra renseigner.	AH RSSI
RO 18 :	Obligatoire	Pour une démarche simplifiée, procéder à une analyse de conformité à partir d'un CUC, formé d'exigences adaptées au périmètre d'homologation et aux besoins de sécurité du SI (socle de sécurité). Alternativement, procéder aux ateliers 1 et 5 de la méthode EBIOS-RM.	RSSI
RO 19 :	Recommandé	Pour une démarche simplifiée, compléter l'analyse de conformité par une analyse de risques lorsque le CUC est insuffisant pour prendre en compte les composants essentiels du périmètre d'homologation ou encore les besoins de sécurité du SI.	RSSI
RO 20 :	Obligatoire	Pour une démarche standard, mener une analyse de risques complète selon la méthode préconisée par le ministère.	RSSI
RO 21 :	Obligatoire	Pour toute démarche standard, réaliser un audit. Les résultats et les actions qui en découlent sont étudiés lors de la commission d'homologation.	RSSI
RO 22 :	Obligatoire	Insérer la décision d'homologation dans l'outil de suivi du patrimoine applicatif du ministère des Armées (sous réserve du niveau de classification de cette décision).	RSSI
RO 23 :	Obligatoire	Prendre une décision d'homologation à l'issue d'une démarche d'homologation. La décision peut être assortie de conditions ou de restrictions d'emploi (temporelles, fonctionnelles) pour une durée déterminée. La démarche peut aussi conduire à un refus d'homologation.	AH
RO 24 :	Obligatoire	Insérer dans la décision d'homologation le niveau de protection maximal des données pouvant être traitées par le SI et leurs éventuelles mentions de manipulation ou de diffusion.	AH
RO 25 :	Obligatoire	Assortir la décision d'homologation d'une durée de validité et fixer les conditions de validité.	AH
RO 26 :	Obligatoire	Remettre en cause une décision d'homologation quand : - les conditions de sa validité ne sont plus respectées ; - les conditions de configuration ou d'exploitation du SI ont été modifiées de manière significative ; - le SI ne correspond plus au périmètre d'homologation (ajout de fonctionnalités, d'applications, d'interconnexions non prévues) ; - des vulnérabilités ont été détectées et peuvent remettre en cause le niveau de sécurité du SI de manière inacceptable ; - les menaces sur le SI ont significativement évolué ; - des problèmes d'application des mesures de sécurité ont été identifiés, notamment lors d'un contrôle ou d'un audit ; - le MCS du SI n'est pas applicable ou suffisamment appliqué, ou a été défaillant ; - le système a fait l'objet d'un incident de sécurité significatif mettant en doute le niveau de sécurité attendu.	AH RSSI AE

N°	Statut (cf. §0)	Intitulé de la règle	Acteur ¹⁷
RO 27 :	Obligatoire	Pour un renouvellement d'homologation, procéder <i>a minima</i> à : - une revue des informations figurant dans le dossier d'homologation ; - une revue des informations d'enrôlement dans l'outil de suivi du patrimoine applicatif du ministère des Armées ; - une vérification des hypothèses de l'analyse de risques ; - une vérification de la pertinence des exigences de sécurité appliquées au SI ; - une revue du PTR; - un bilan des contrôles et audits réalisés sur le SI ; - un bilan de l'activité liée au MCS pour évaluer sa performance et identifier les événements marquants.	AH RSSI
RO 28 :	Obligatoire	Pour homologuer un SI déclaré d'importance vitale, mener une démarche d'homologation de type standard. Toute dérogation à cette règle nécessite l'autorisation formelle du FSSI.	AH RSSI
RO 29 :	Obligatoire	Traiter et protéger la décision d'homologation et le dossier d'homologation d'un SIIV <i>a minima</i> comme des documents de niveau de confidentialité DIFFUSION RESTREINTE et SPÉCIAL FRANCE. Selon les éléments qu'ils contiennent, ils peuvent être classifiés.	AH RSSI
RO 30 :	Interdit	Ne pas enrôler les SIIV dans un outil non classifié si celui-ci mentionne sa catégorisation de SIIV.	AH RSSI
RO 31 :	Obligatoire	Dans le cas de l'homologation d'un système traitant d'informations classifiées TRÈS SECRET faisant l'objet d'une classification spéciale, saisir formellement le HFCDS du lancement de toute démarche d'homologation, l'AH étant dans ce cas le SGDSN.	AE RSSI
RO 32 :	Obligatoire	Mettre en destinataire des décisions d'homologation de SI classifié, le FSSI et l'ANSSI.	AH
RO 33 :	Obligatoire	Procéder à une démarche standard pour homologuer des SI classifiés contenant des matériels et logiciels agréés à un niveau inférieur exigé ou non-agréés. L'AH justifie l'autorisation de leur utilisation. La justification est insérée dans le dossier d'homologation. La règle ne s'applique pas pour une homologation d'un dispositif d'interconnexion ou d'un segment d'interface. Toutefois, sur proposition de son CEAH, une AH peut décider de déroger à la règle sous certaines conditions.	AH RSSI
RO 34 :	Obligatoire	Préciser sur la décision d'homologation que le SI traitant des données à caractère personnel est apte pour en assurer la protection lorsque ce traitement donne lieu à un acte réglementaire.	AH
RO 35 :	Conseillé	Dans des cas d'urgences politique, stratégique ou opérationnelle, instruire de préférence une première décision d'homologation formelle plutôt qu'une homologation sous réserves.	AH
RO 36 :	Obligatoire	Préciser formellement dans la stratégie d'homologation du SI de référence la procédure de l'homologation de déploiement ainsi que les différents responsables et les livrables attendus.	RSSI
RO 37 :	Obligatoire	Pour le RSSI du SI de référence, suivre ses déploiements et leur état d'homologation. Il coordonne les différentes démarches d'homologation de déploiement.	RSSI
RO 38 :	Obligatoire	Pour une homologation de déploiement, y compris dérogatoire, appuyer la décision d'homologation du SI déployé sur des CUC et des PES locales.	AH
RO 39 :	Interdit	De renouveler plus d'une fois une HDD.	AH

N°	Statut (cf. §0)	Intitulé de la règle	Acteur ¹⁷
RO 40 :	Obligatoire	Lors d'un renouvellement d'homologation du SI de référence, procéder au renouvellement des homologations de déploiements liées à la précédente décision d'homologation.	AH
RO 41 :	Obligatoire	Pour tout hébergeur relevant du ministère, avertir les autorités clientes ou d'emploi des SI qu'il héberge de tout élément, dysfonctionnement ou incident pouvant remettre en cause leur niveau de sécurité.	Hébergeur
RO 42 :	Obligatoire	Homologuer les systèmes ou services numériques fournis par un prestataire de service d'informatique en nuage pour traiter des données relevant du ministère des Armées selon un périmètre d'homologation défini en fonction de la nature du service rendu ou du produit fourni.	AE AH
RO 43 :	Obligatoire	Pour le prestataire d'informatique en nuage externalisé, fournir un PAS. Le PAS produit par le prestataire est alors inséré dans le dossier d'homologation.	RSSI
RO 44 :	Obligatoire	Considérer dans le périmètre d'homologation l'utilisation et le cadre d'utilisation du service <i>IaaS</i> ou <i>PaaS</i> tant dans sa dimension fonctionnelle que sécuritaire.	RSSI
RO 45 :	Obligatoire	Pour l'AE, fournir une appréciation d'usage à l'AH avant d'initier la démarche d'homologation portant sur l'usage du service numérique.	AE
RO 46 :	Obligatoire	Pour l'AE, établir une politique d'emploi pour pouvoir utiliser un service numérique public de type <i>SaaS</i> . Elle est fournie à l'AH pour insertion dans le dossier d'homologation.	AE
RO 47 :	Recommandé	Pour une homologation d'un système de systèmes, procéder à une analyse de risques portant non seulement sur chacun de ses composants mais également sur l'ensemble du système de systèmes et l'interdépendance de ces derniers.	RSSI
RO 48 :	Obligatoire	Pour toute interconnexion de SI de niveaux de classification différents ou entre un SI classifié et un SI non-classifié, la justifier formellement auprès de l'AH et de l'AQSSI par un besoin opérationnel.	AE
RO 49 :	Obligatoire	Procéder à une homologation spécifique des interconnexions ou de segments d'interface de SI de même niveau de classification. L'interconnexion ou le segment d'interface de SI est alors homologué au même niveau de classification que ces systèmes.	AH
RO 50 :	Obligatoire	Procéder à une homologation spécifique des dispositifs d'interconnexion ou des segments d'interface de SI de niveaux de sensibilité ou de classification différents, ou de SI externes au ministère des Armées. L'interconnexion ou le segment d'interface de SI est alors homologué au niveau du SI le plus élevé.	AH
RO 51 :	Recommandé	Procéder à une homologation spécifique des dispositifs d'interconnexion ou des segments d'interface de SI non classifiés et relevant du ministère des Armées.	AH
RO 52 :	Obligatoire	Dans le cadre d'un développement de SI en mode agile, mentionner dans la stratégie d'homologation les modalités des échanges entre les différents acteurs (RSSI, équipe de développement, CEAH), le rythme des remontées d'informations ainsi que les conditions de maintien de l'homologation.	RSSI
RO 53 :	Obligatoire	Subordonner la mise en exploitation d'un SI pour test ou expérimentation à l'autorisation formelle de l'AH qui valide les conditions de sécurité préalablement définies. Dans le cadre d'un test, la stratégie d'homologation doit prévoir cette autorisation et en préciser les modalités. L'autorisation d'exploitation est associée à une date de fin de validité et à un niveau de confidentialité des données à traiter.	RSSI

ANNEXE 5. CADRE DOCUMENTAIRE

Documents et ressources applicables

[Audit]	[2013-10-23] Directive n°28/DEF/DGSIC du 23/10/2013 portant sur l'exécution des audits	Intradef
[BASECASSIS]	Pack homologation de la DGA	Intradef
[CLOUD État]	[2021-07-05] Circulaire n°6282/SG du 5/07/2021 relative à la doctrine d'utilisation de l'informatique en nuage par l'État (« cloud au centre »)	Internet
[CLOUD SaaS]	[2022-07-18] Politique d'hébergement des SI et des données sur Internet, note N°255/ARM/DGNUM/SDTN/NP du 18 juillet 2022	Intradef
[DEFEND]	[2016-09-06] Note n°D-16-008326/DEF/EMA/SCOPS/CYBER/DR du 6/09/2016 relative à la défendabilité des SI	Intradef
[DIR 39]	[2016-07-01] Directive n°39/DEF/DGSIC/DR de 1/07/2016 relative à la sécurité des systèmes industriels (2^{ème} édition, approuvée le 9 juin 2023)	Intradef
[GUIDE 7]	[2020-11-19] Guide n°7 portant sur l'intégration de la sécurité numérique dans le cycle de vie d'un système d'information, note n°443/ARM/DGNUM/DG/NP	Intradef
[KIT RSSI COMCYBER]	Kit RSSI du COMCYBER, portant des informations et des outils relatifs à la démarche d'homologation	Intradef
[KIT RSSI SGA]	SGA-MSI RSSI AQ SGA - Accueil (Demander soumise à autorisation auprès du SGA : sga.raq-ossi.fct@intradef.gouv.fr)	Intradef

	[GUIDE HYG]	[2017-01-23] Guide d'hygiène informatique - ANSSI	Internet
	[GUIDE S2I]	[2025-11-27] Maîtriser la SSI pour les systèmes industriels - ANSSI	Internet
	[GUIDE SSI]	Ensemble des guides [GUIDE HYG] et [GUIDE S2I]	Internet
	[IGI 1300]	[2021-08-09] Instruction générale interministérielle n°1300 sur la protection du secret de la défense nationale du 9/08/2021	Intraderf
	[II 901]	[2015-01-28] Instruction interministérielle n°901/SGDSN/ANSSI relative à la protection des systèmes d'information sensibles	Intraderf
	[IM DAJ-RGPD]	[2020-01-31] Instruction ARM/SGA/DAJ/D2P du 31/01/2020 relative à la mise en œuvre du règlement européen sur la protection des données personnelles au ministère de la défense	Intraderf
	[LID]	[2018-12-01] Instruction ministérielle n°101000/ARM/CAB du 1/12/2018 relative à la politique de lutte informatique et défensive du ministère des Armées	Intraderf
	[MCS]	[2020-06-04] Directive n°47 portant sur le maintien en condition de sécurité, note n°200/ARM/DGNUM/DG/DR du 4/06/2020	Intraderf
	[PMSN-S]	[2026-01-05] Instruction ministérielle n°500168/ARM/CAB/CM3 du 05 janvier 2026 relative au volet stratégique de la politique ministérielle de la sécurité numérique	Intraderf
	[PSSIM-T]	[2021-07-21] Instruction ministérielle n°7362-2/ARM/CAB du 21/07/2021, édition 2, portant sur le volet technique de la politique de sécurité du système d'information du ministère des Armées	Intraderf

[RGS]	[2014-06-13] Référentiel Général de Sécurité, version 2.0 du 13/06/2014	Internet
[RGI]	[2016-04-20] Référentiel Général d'Interopérabilité, version 2 du 20/04/2016	Internet
[SIIV]	[2021-03-22] Arrêté du 22/03/2021 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'importance vitale « Activités militaires de l'État »	Internet
[Traces]	[2013-11-12] Directive n°29/DEF/DGSIC du 12/11/2013 relative aux traces et leur gestion au sein du ministère de la Défense	Intradef

Documents et sites de référence complémentaires

[EBIOS RM]	[2018-10-09] Expression des Besoins et Identification des Objectifs de Sécurité - Risk Manager - ANSSI	Internet
[FICHE 2 DCP]	[2019-08-08] Fiche n°2 de la direction des affaires juridiques portant sur l'AIPD et les actes réglementaires portant création du traitement des données	Intraderf
[MAITRISK]	[2020-07-02] Directive n°45/ARM/DGNUM/SDSNUM/DR relative à l'emploi de l'outil « MAITRISK » au ministère des Armées	Intraderf
[Site ANSSI]	Site de l'ANSSI	Internet
[GUIDE HOMOLOG]	[2025-04-01] Guide de l'homologation de sécurité des systèmes d'information - Version 2.0 - ANSSI	Internet
[SI ISOLE]	[2025-04-01] Guide d'homologation de sécurité des systèmes d'information de l'ANSSI. Fiche méthode « SI isolé et simple », version 1.0	Internet
[SUPERVISION]	[2025-07-25] Guide Anssi supervision	Internet