BULLETIN OFFICIEL DES ARMEES

Edition Chronologique n°9 du 22 février 2013

PARTIE PERMANENTE
Administration Centrale

Texte n°2

DIRECTIVE N° 27/DEF/DGSIC
portant sur l'homologation des systèmes d'information du ministère de la défense.

Du *24 janvier 2013*

DIRECTION GÉNÉRALE DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION.

DIRECTIVE N° 27/DEF/DGSIC portant sur l'homologation des systèmes d'information du ministère de la défense.

Du 24 janvier 2013

NOR D E F E 1 3 5 0 0 6 0 X

Pièce(s) Jointe(s) :

Onze annexes et trois appendices.

Classement dans l'édition méthodique : BOEM 160.1

Référence de publication : BOC N°9 du 22 février 2013, texte 2.

SOMMAIRE

ANNEXE(S)

1. PRÉSENTATION GÉNÉRALE ET GUIDE D'USAGE.

1.1. **Présentation.**

La présente directive définit la politique à mettre en œuvre en matière d'homologation de sécurité pour les systèmes d'information (SI) au sein du ministère de la défense. Elle fournit les critères de décision pour mener à terme toute démarche d'homologation, permettant ainsi d'identifier, d'atteindre, puis de maintenir un niveau de risque acceptable, tant du point de vue de la sécurité que des coûts. Elle concerne tous les SI du ministère, quel que soit le niveau de sensibilité des informations traitées.

Les éléments techniques, comme l'homogénéisation des documents, figurent en annexe et appendice.

Cette directive s'inscrit dans les missions de la direction générale des systèmes d'information et de communication (DGSIC), aux termes du décret n° 2006-497 du 2 mai 2006 modifié, portant création de la direction générale des systèmes d'information et de communication et fixant l'organisation des systèmes d'information et de communication du ministère de la défense.

Elle tient compte des dispositions des différents textes réglementaires [référentiel général de sécurité (RGS) version 1.0 du 6 mai 2010 (1), instruction générale interministérielle n° 1300/SGDSN/PSE/SSD du 30 novembre 2011 (1) sur la protection du secret de la défense nationale, instruction ministérielle n°

900/DEF/CAB/-- du 26 janvier 2012 (1) (IM 900) relative à la protection du secret de la défense nationale au sein du ministère de la défense, etc.] et des retours d'expérience en matière d'homologation de systèmes nationaux.

1.2. **Niveaux de préconisation.**

Les règles définies dans ce document ont différents niveaux de préconisation et sont conformes au référentiel général d'intéropérabilité (RGI) et à la *request for comment* (RFC) 2119 :

- 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 ;

- 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 le cas soigneusement pesé ;

- interdit : ce niveau de préconisation signifie que la règle édictée indique une prohibition absolue de la directive.

1.3. **Champs et modalités d'application.**

Cette directive est applicable aux organismes du ministère de la défense, au sens de l'instruction générale interministérielle sur la protection du secret de la défense nationale (1) (IGI 1300). Elle fait partie de la politique de sécurité de tout SI.

L'homologation de sécurité d'un système est globale : elle inclut dans son périmètre tout ce qui peut avoir un impact sur la sécurité du système, de nature technique ou organisationnelle.

Son cadre d'exécution doit préciser son champ d'action, son organisation, les responsabilités des acteurs, et la démarche d'homologation proprement dite.

La directive est complétée du guide ministériel relatif à l'intégration de la sécurité des systèmes d'information (SSI) dans les projets de SI [guide n° 7 du 6 janvier 2012 (1) relatif à l'intégration de la sécurité des systèmes d'information dans les projets de systèmes d'information, 1re édition].

Cette directive sera appliquée dès sa parution pour les nouveaux systèmes.

Pour les systèmes déjà en exploitation et non homologués, chaque autorité qualifiée (AQ) présentera en commission ministérielle de la sécurité des systèmes d'information (CMSSI), en fonction du nombre des SI et des moyens à consacrer, une feuille de route synthétique permettant leur mise en conformité dans des délais raisonnables.

1.4. **Gestion des dérogations aux règles de la directive.**

Les dérogations font l'objet d'une approbation par l'AQ concernée ou son représentant. Elles concernent les circonstances et justifications du non respect d'une règle.

Un bilan annuel synthétique des dérogations pourra être demandé à chaque AQ en CMSSI.

2. CADRE DOCUMENTAIRE.

2.1. **Documents applicables.**

CP	:	code pénal. http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719. http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719.
CNIL	:	loi n° 78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460.
RGI	:	référentiel général d'interopérabilité du 12 mai 2009 (1), version 1.0. http://references.modernisation.gouv.fr/rgi-interoperabilite.
RGS	:	référentiel général de sécurité du 6 mai 2010 (1), version 1.0. http://www.references.modernisation.gouv.fr/rgs-securite.
IGI 1300	:	instruction générale interministérielle n° 1300/SGDSN/PSE/SSD du 30 novembre 2011 (1) sur la protection du défense nationale. http://www.ssi.gouv.fr/reglementation-ssi/systemes-d-information/.
II 155	:	instruction interministérielle nº 155/SGDSN/AIST/PST/-- du 7 novembre 2012 (1) sur la protection du patrimoine et technique dans les échanges internationaux.
PSSI	:	instruction n° 133/DEF/SEC/DIR/SIC du 18 mars 2002 modifiée, relative à la politique de sécurité des systèmes d' du ministère de la défense. http://synoptic.intradef.gouv.fr/sites/default/files/16f143a5d01.pdf (intranet).
IM 900	:	instruction ministérielle n° 900/DEF/CAB/-- du 26 janvier 2012 (1) relative à la protection du secret de la défense sein du ministère de la défense. http://synoptic.intradef.gouv.fr/sites/default/files/55308737d01.pdf (intranet).
IG 125/1516	:	instruction générale n° 125/DEF/EMA/PLANS/COCA - n° 1516/DEF/DGA/DP/SDM du 26 mars 2010 relative au et la conduite des opérations d'armement, tome I.
NOTE 1979	:	note n° 1979/ANSSI du 28 juillet 2010 (1) sur la délégation du pouvoir d'homologation à l'état-major des armées.
NOTE	:	rôles et responsabilités relatifs à la conduite du processus d'homologation des systèmes traitant des informations cla nationales (version provisoire) - ANSSI.
EBIOS	:	expression des besoins et identification des objectifs de sécurité - ANSSI. http://www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/ebios-expression-des-besoins-et-identification -des-objectifs-de-securite.html.
FEROS	:	fiche d'expression rationnelle des objectifs de sécurité des systèmes d'information - guide tec 150/SGDN/DISSI/SCSSI du 10 février 1991 (1). http://www.ssi.gouv.fr/IMG/pdf/ebiosv2-mp-feros-2005-0418.pdf. http://www.ssi.defense.gouv.fr/_dirsic/textes/mis_sec_dir_sic/secur_sys_info/textes_base/ref_regl/textes _nationaux_europeens/textes_intermin_guides/guide_n__150.pdf.
M@RGERIDE	:	méthode d'analyse rapide et de gestion évolutive des risques dérivée d' http://www.dgsic.defense.gouv.fr/sites/default/files/20120216_NP_DGSIC_SDSSI_NO-221-Margeride.pdf.
PROC AGR	:	processus d'agrément des produits de sécurité à usage gouvernemental n° 1047/SGDN/DCSSI/-- (2003) (1).
GUIDE 007	:	guide n° 7 du 6 janvier 2012 (1) relatif à l'intégration de la sécurité des systèmes d'information dans les projets d'information, 1re édition. http://synoptic.intradef.gouv.fr/ressource-documentaire/guide-ndeg7defdgsic-relatif-l-integration-de-la-ssi-dans-les-p (intranet).
RFC 2119	:	*request for comment* - mots clés à utiliser dans les RFC pour indiquer les niveaux d'e http://www.ietf.org/rfc/rfc2119.txt.

2.2. **Sites de référence.**

Sites SSI :

- site SSI de l'ANSSI (agence nationale de la sécurité des systèmes d'information) à l'adresse internet : http://www.ssi.gouv.fr ;

- site SSI du ministère à l'adresse intradef : http://synoptic.intradef.gouv.fr/ssi.

3. DOMAINE COUVERT ET EMPLOI.

La directive vise à définir les principes et les démarches à suivre pour toute homologation d'un SI relevant des autorités qualifiées du ministère de la défense.

3.1. **Principes fondamentaux.**

La démarche d'homologation est une composante de la gestion de la sécurité réalisée tout au long du cycle de vie d'un SI.

3.1.1. ***Fondements.***

L'homologation est une des responsabilités de l'autorité qualifiée en SSI (AQSSI). Une AQ peut déléguer le suivi de la démarche ou les décisions d'homologation à une ou plusieurs autorités d'homologation (AH), principales ou secondaires. La délégation donnée à l'AH par l'AQ ne transfère pas sa responsabilité.

Les modalités d'application de cette directive à un système particulier sont approuvées par l'AH pour chaque système, en tenant compte en particulier du type de système et de la réglementation en vigueur.

La décision d'homologation de sécurité est l'acte formel par lequel l'AH certifie, après évaluation des risques et analyse des mesures de sécurité mises en œuvre, que la protection des informations et du système est assurée au niveau requis. Elle est un préalable à l'autorisation d'exploitation.

Dans tous les cas, l'homologation traduit l'acceptation des risques du système considéré dans un environnement donné.

Elle est prononcée pour une certaine durée et sous condition de non évolution majeure des hypothèses, des risques et des vulnérabilités afférents au système. Elle doit donc être régulièrement reconsidérée tout au long de la vie du système.

La démarche d'homologation conduit l'AH à déclarer, à la vue du dossier d'homologation (composition en appendice), que le SI considéré est apte à traiter des informations conformément aux objectifs de sécurité visés, et que les risques résiduels induits sont pris en compte et acceptés.

La démarche d'homologation s'inscrit dans le cycle de vie d'un système et s'appuie sur :

- l'identification des besoins et des objectifs de sécurité ;

- une gestion globale des risques de sécurité concernant l'ensemble du SI tout au long de son cycle de vie ;

- la mise en œuvre d'une méthode d'analyse de risques éprouvée, et l'examen des informations qu'elle fournit ;

- l'évaluation des mesures de sécurité à mettre en œuvre ;

- la vérification des conditions de mise en œuvre des mesures de sécurité ;

- la définition et la mise en œuvre des processus de maintien en condition de sécurité ;

- l'examen des risques résiduels et l'évaluation des processus permanents de gestion des risques.

3.1.2. ***Évolutions.***

La capitalisation des retours d'expérience et la prise en compte des modifications des textes de référence permettront de faire évoluer et d'adapter cette directive, en tenant compte des points suivants :

- définition d'une démarche structurée, capable d'assurer qu'un niveau de protection suffisant du SI sera atteint et maintenu ;

- mise en œuvre et suivi de la démarche établie, tout au long du cycle de vie du SI ;

- vérification du niveau de protection atteint et engagement de son maintien pendant tout le cycle de vie du SI.

Les modalités de cette capitalisation seront fixées par la DGSIC.

3.2. **Vue d'ensemble.**

Tout système d'information doit être homologué.

Cependant, tout SI ne présente pas les mêmes enjeux de sécurité en matière de confidentialité des données, d'intégrité, de disponibilité et de criticité pour les missions du ministère. De plus, de nombreux SI ou applications sont hébergés sur les intranets du ministère bénéficiant, ainsi, des services de sécurité apportés par ces réseaux : c'est la notion d'héritage. Notamment, mais pas seulement, les mesures de protection apportées par les environnements de sécurité [*global security environment* (GSE), *local security environment* (LSE)] du SI d'accueil seront considérées, *de facto*, acquises pour les applications ou SI installées.

Dans ces conditions, la DGSIC a développé, en complément de la démarche d'homologation standard, deux méthodes d'homologation qui permettent de restreindre et de simplifier le processus d'homologation.

La démarche sommaire d'homologation correspond à une fiche descriptive de la sécurité du système. Elle se présente comme un simple énoncé des mesures de sécurité techniques et organisationnelles (sans analyse de risque). Elle est réservée aux applications, voire SI, ne traitant pas d'informations classifiées de défense et ne présentant pas de besoin particulier en matière de disponibilité, d'intégrité ou de traçabilité.

La démarche d'homologation simplifiée est essentiellement orientée autour de la production des exigences de sécurité et des contre-mesures prises (dossier de sécurité). Les exigences de sécurité sont obtenues aisément grâce à un outil d'analyse automatique de risques, basée sur une mesure de la conformité du SI par rapport à la réglementation et aux bonnes pratiques SSI existantes. De plus, une grande partie des contre-mesures (apportées par le réseau ou SI d'accueil) peuvent être couvertes par la notion d'héritage.

Un processus d'auto-évaluation rapide permet de distinguer les systèmes qui peuvent relever d'une démarche sommaire ou simplifiée de ceux pour lesquels une démarche standard s'impose. Le bilan du questionnaire est validé par l'AH.

Dans les trois cas, l'homologation traduit l'acceptation des risques du système considéré dans un environnement donné.

Cette gestion des risques se traduit par un choix de démarche adaptée au niveau de sécurité.

La démarche initiale amène à une homologation de référence.

Dans le cas de l'extension du périmètre d'homologation de référence (prévu ou non), chaque déploiement fera l'objet d'une homologation liées au(x) déploiement(s).

Cette méthode est notamment adaptée pour les systèmes utilisés en opération extérieure (OPEX) (dont les conditions de déploiement ne peuvent être connues à l'avance, mais qui peuvent être anticipées, contrôlées et validées en exercice) ou pour des systèmes déployés sur de nombreux sites (et pour lesquels il peut être souhaitable de prononcer l'homologation avant la fin du déploiement complet sur tous les sites).

Dans le cadre de cette démarche, l'homologation est basée, d'une part, sur la certification de la conformité du site et de l'environnement de sécurité (GSE, LSE) et, d'autre part, sur la conformité de l'installation du SI [qui

inclut les parties réseau et configuration des stations de travail - *electronic security environment* (ESE)] par rapport aux exigences incluses dans l'homologation du système de référence (2).

Il s'agit de valider le respect des objectifs génériques de sécurité du système de référence et de limiter les travaux sur un site particulier au contrôle de la conformité du déploiement par rapport aux impératifs de sécurité portant sur l'environnement du système et sa configuration (homologation du SI déployé).

L'autorité d'homologation est responsable devant l'autorité qualifiée du maintien du niveau de sécurité du système. Elle s'assure *via* la voie fonctionnelle SSI que le SI fonctionne avec le niveau de sécurité accepté lors de son homologation et que les conditions de sécurité fixées sont maintenues. Pour mémoire, le plan de contrôle est défini au sein de la stratégie d'homologation. Il peut consister en un simple audit de conformité réalisé ou diligenté par le responsable de sécurité des systèmes d'information (RSSI) désigné (3) ou en un audit réalisé par une équipe spécialisée.

La commission d'homologation fait préparer le renouvellement de l'homologation ou le lancement des nouvelles démarches d'homologation et peut proposer un audit de sécurité.

3.3. **Périmètre et limites.**

La directive fait partie du référentiel documentaire sur lequel s'appuie la politique de sécurité des SI considérés. En fonction des ressources humaines affectées, des priorités seront à établir.

La directive vise à définir les principes et les démarches à suivre pour toute homologation d'un SI relevant des organismes du ministère de la défense.

Pour des systèmes traitant d'informations sensibles relevant du patrimoine scientifique et technologique (PST), il sera fait référence à l'II 155 (1).

4. LES RÈGLES.

La directive est déclinée sous deux angles : organisationnel (RO) et technique (RT). Les règles sont numérotées séquentiellement par catégorie.

4.1. **Organisation - responsabilités.**

RO 1 : il est obligatoire de n'avoir qu'une AH pour chaque système.

Nota. Cela prend en compte le cas des meta systèmes dont l'homologation nécessite que d'autres systèmes sous-jacents le soient également. Dans ce cas, un partitionnement d'homologation peut être envisagé [logique de SI (intradef et ses applications) ou logique de champs d'action ou d'emploi (théâtres, métropole, outremer etc.)].

RO 2 : il est obligatoire, dans le cas d'une homologation standard ou simplifiée, que l'autorité d'homologation constitue une commission d'homologation, adaptée au cas par cas, selon le système à homologuer et en fixe les règles générales de fonctionnement.

Nota. Pour une homologation sommaire, la constitution d'une commission est à discrétion de l'AH. Le dossier pourra être présenté directement à la signature de l'AH selon une procédure définie par l'AQ.

Par ailleurs dans le cadre d'exercices ou d'opérations, seule l'homologation de référence du SI est soumise à cette règle. Pour le ou les déploiements (4) du système, le dossier pourra être présenté directement à l'AH après signature des certificats de conformité ESE et GSE/LSE par le responsable du site, selon une procédure à déterminer par l'AQ.

RO 3 : il est obligatoire, dans le cas d'une démarche d'homologation standard, que la commission d'homologation soit au minimum composée des acteurs suivants :

- autorité d'homologation ou son représentant ;

- responsable SSI de projet ;

- directeur de projet ;

- représentant de l'autorité d'emploi.

Le fonctionnaire de sécurité des systèmes d'information (FSSI) et l'AQ peuvent participer à toute commission d'homologation et donc accéder à l'ensemble des informations du dossier d'homologation.

Nota. Certains acteurs peuvent cumuler plusieurs des rôles définis *supra*. Dans le cas d'une démarche sommaire ou simplifiée, la composition de la commission est réduite.

4.2. **Homologation de sécurité.**

RO 4 : il est obligatoire que tout SI fasse l'objet d'une homologation ou d'une autorisation provisoire d'exploitation (APE) avant sa mise en service opérationnel.

Nota. Cette règle prend en compte les modalités définies au point 1.3.

RO 5 : il est recommandé d'appliquer la méthode d'auto-évaluation rapide de son niveau adéquat d'objectif SSI afin de déterminer le type de démarche d'homologation à engager (standard, simplifié ou sommaire).

RO 6 : il est obligatoire d'appliquer l'une des trois démarches d'homologation identifiées (sommaire, simplifiée, standard), selon la décision de l'autorité qualifiée.

RO 7 : il est obligatoire, pour les homologations liées à un déploiement et une fois l'homologation de référence prononcée, que les opérations de conformité des sites opérationnels soient préparées par le responsable SSI désigné (3) et validées par l'autorité du site.

Nota. Les opérations de conformité (ou audit de conformité) consistent à vérifier que les mesures de sécurité organisationnelles, physiques et techniques décrites au sein de la procédure d'exploitation de la sécurité (PES) du système de référence sont bien appliquées et déclinées si nécessaires au sein de la PES de l'instance déployée. Elles se réalisent avec l'aide des acteurs en charge de la sécurité physique. L'autorité du site s'engage donc formellement sur le niveau global de sécurité atteint.

RO 8 : il est obligatoire dans le cadre d'une homologation de référence, de préciser formellement les conditions de délégation pour le déploiement.

Nota. Ces conditions sont inscrites dans la stratégie d'homologation.

RO 9 : il est obligatoire dans le cas de l'homologation d'un système traitant d'informations classifiées « très secret défense » de saisir formellement le haut fonctionnaire correspondant de défense et de sécurité (HFCDS) du lancement de toute démarche d'homologation, l'autorité d'homologation étant dans ce cas le secrétariat général de la défense et de la sécurité nationale (SGDSN).

Nota. Dans ce cas, c'est une déclaration d'aptitude qui est établie et envoyée au SGDSN.

4.3. **Documentation.**

RT 1	:	il est recommandé d'utiliser les modèles de documents décrits en annexes.
RT 2	:	il est recommandé que la documentation liée aux homologations soit accessible depuis l'outil métier (5) de la SSI, dans la limite du niveau de protection apporté par l'application.
RO 10	:	il est obligatoire, afin que la décision d'homologation soit motivée et justifiée, que la commission d'homologation s'appuie sur un dossier d'homologation (6).

RO 11 : il est obligatoire, pour la démarche d'homologation standard, d'établir une stratégie d'homologation, approuvée par l'AH.

4.4. **Démarche d'homologation.**

RO 12 : il est recommandé de suivre et de conduire toute démarche d'homologation à l'aide de l'outil métier de la SSI.

RO 13 : il est obligatoire, avant la phase de réalisation, de faire valider par l'AH les orientations techniques permettant de répondre aux exigences de sécurité.

4.5. **Homologation et livrables système de sécurité informatique.**

RO 14 : il est recommandé, afin de garantir une cohérence entre les validations fonctionnelles et SSI, de conditionner chaque passage d'une étape d'une démarche d'homologation à l'approbation des livrables SSI exigés.

4.6. **Périmètre et stratégie d'homologation.**

RO 15 : il est obligatoire de procéder à une homologation spécifique des segments d'interfaces reliant deux SI de niveaux différents de sensibilité, ou de l'interface avec des systèmes extérieurs au ministère.

RO 16 : il est obligatoire, dans la stratégie d'homologation, de faire figurer dans les pièces de référence le document qui détaille la stratégie de gestion des risques [démonstration de couverture, identification des risques non couverts, maîtrise des risques, etc. (7)].

RO 17 : il est obligatoire d'homologuer toute extension du périmètre de l'homologation initiale.

RT 3 : il est obligatoire, lors de la définition du périmètre de l'homologation, de tenir compte au minimum :

- des interconnexions avec d'autres systèmes ;
- des homologations nécessaires et préalables à l'homologation à obtenir ;
- des supports amovibles ;
- des accès à distance par des utilisateurs « nomades » ;
- des conditions de maintien en condition de sécurité ;
- des opérations de maintenance, d'exploitation ou de télégestion du système, notamment lorsqu'elles sont effectuées par des prestataires externes ;
- de la fourniture d'extrait de la base de données ;
- de la formation des utilisateurs et des administrateurs.

RT 4 : il est obligatoire de constituer le dossier d'homologation avec, *a minima*, les pièces mentionnées dans l'annexe V.

4.7. **Décision d'homologation.**

Lors de l'instruction d'un dossier d'homologation, il peut être constaté qu'un système ne remplit pas les conditions techniques nécessaires à son homologation.

L'AH peut toutefois apprécier le risque pris en cas de mise en service opérationnel du système pour une durée limitée et considérer ce risque comme acceptable. Elle prononce alors une APE assortie d'une condition explicite :

- soit de retrait du service à l'issue de l'APE ;

- soit de correction des faits constatés en vue d'une homologation en bonne et due forme.

RO 18 : il est obligatoire que toute démarche d'homologation amène à l'une des décisions suivantes :

- homologation assortie le cas échéant de conditions, pour une durée déterminée ;

- refus d'homologation.

RO 19 : il est obligatoire d'assortir l'homologation ou l'APE d'une durée de validité laissée à l'appréciation de l'autorité d'homologation. Cette durée ne doit pas dépasser (8) :

- 6 mois renouvelable une fois pour une autorisation provisoire d'exploitation ;

- 2 ans pour les systèmes traitant des informations classifiées au moins « secret défense » ;

- 5 ans pour les systèmes traitant des informations classifiées « confidentiel défense » ;

- 5 ans pour des systèmes traitant des informations sensibles non classifiées de défense ;

- 7 ans pour les autres systèmes nationaux.

RO 20 : il est obligatoire de formaliser toute décision d'homologation par un document écrit, avec ou sans contrainte.

RT 5 : il est obligatoire, dans le cas d'une autorisation provisoire d'exploitation, de fixer les conditions de sa validité, en précisant notamment :

- le relevé et l'échéancier des actions à mener en vue de l'homologation ;

- les éventuelles restrictions d'emploi temporaires.

RT 6 : il est obligatoire, pour toute homologation, de fixer les conditions de sa validité, en précisant notamment :

- les éventuelles restrictions d'emploi temporaires ;

- les risques résiduels acceptés ;

- les conditions de retrait du système.

4.8. **Contrôle et renouvellement d'homologation.**

RT 7 : il est obligatoire que le RSSI fasse une analyse d'impact sur la sécurité du SI lorsque :

- les conditions d'exploitation du système ont été modifiées ;

- des nouvelles fonctionnalités ou applications doivent être installées ;

- le système a été interconnecté à de nouveaux systèmes ;

- des problèmes d'application des mesures de sécurité ou des conditions de maintien de l'homologation ont été révélés, par exemple lors d'un audit de sécurité [niveau de criticité à déterminer avec les acteurs de la lutte informatique défensive (LID)] ;

- l'appréciation des menaces sur le système a évolué de façon majeure ou les réponses à la méthode d'auto-évaluation rapide sont modifiées, conduisant à un changement de démarche d'homologation préconisée ;

- de nouvelles vulnérabilités ont été découvertes (à partir d'un certain niveau de criticité à déterminer avec les acteurs LID) ;

- le système a fait l'objet d'un incident de sécurité (à partir d'un certain niveau de criticité à déterminer avec les acteurs LID).

Lorsqu'un impact sur la sécurité est constaté, le RSSI convoque la commission d'homologation pour statuer sur la remise en cause de l'homologation du système.

Nota. La commission d'homologation se réunit pour statuer sur l'homologation.

Les acteurs LID sont identifiés dans la note n° 59/DEF/EMA/SC_OPS/CYBER/-- du 16 décembre 2011 (1) relative à l'organisation « lutte informatique défense » : préparation des engagements en cas de crise cybernétique et des contrats opérationnels afférents.

Pour le ministre de la défense et par délégation :

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

Gérard LAPPREND.

---

(1) n.i. BO.

(2) Il est à noter que le principe de certificat de conformité peut être appliqué dans le cadre de la démarche d'homologation d'un SI pour certifier conforme tout ou partie du SI à un SI dit référent, déjà homologué. Dans ces conditions la (ou les) décision de certification de conformité est insérée comme pièce justificative au dossier d'homologation du SI. En effet, elle ne se substitue pas à la décision d'homologation de responsabilité de l'AH.

(3) Officier de la SSI local (OSSI-L), correspondant(s) de sécurité des systèmes d'information (CSSI) ou officier de la SSI territorial (OSSI-T).

(4) Il peut y avoir plusieurs instances de déployées pour un même système de référence.

(5) Il faut souligner que cet outil n'est pas actuellement encore choisi.

(6) Pour une démarche d'homologation dite sommaire ce dossier peut se résumer à une fiche descriptive.

(7) Généralement appelé le plan de sécurité (PDS) ou la cible de sécurité (CDS).

(8) Conformément au point 6.3.3. de l'[IM 900].

ANNEXE I.

GLOSSAIRE ET ACRONYMES.

Agrément d'un produit de sécurité	:	reconnaissance formelle que le produit de sécurité évalué peut protéger des informations jusqu'à un niveau spécifié dans les conditions d'emploi définies.
APE	:	autorisation provisoire d'exploitation.
Autorité d'emploi	:	autorité qui est à l'origine du besoin du SI. Elle est également responsable de la mise en œuvre du SI. C'est l'autorité d'emploi, qui après avoir défini les finalités du traitement en pilote l'emploi et les évolutions. Elle est le garant de la bonne utilisation du SI. Elle pilote l'emploi et les évolutions sous couvert de l'AH.
Autorité d'exploitation (AE)	:	autorité qui assure les fonctions techniques d'exploitation du système d'information [exemple : direction interarmées des réseaux d'infrastructure et des systèmes d'information (DIRISI)].
Autorité d'homologation (AH)	:	autorité de niveau hiérarchique suffisant désignée par l'autorité qualifiée qui, sur avis d'une commission d'homologation, signe la décision autorisant l'emploi d'un SI. Cette compétence en matière d'homologation peut être déléguée à une autorité déléguée. La délégation fixe alors les limites des attributions correspondantes et précise le niveau de confidentialité maximal pour lequel chaque autorité déléguée est compétente.
Autorité qualifiée en matière de SSI (AQ SSI)	:	responsable de la sécurité des systèmes d'information dans les administrations centrales et les services déconcentrés de l'État, dans les établissements publics, placé sous l'autorité d'un ministre ainsi que dans les organismes et établissements relevant de ses attributions.
Besoin de sécurité	:	définition précise et non ambiguë des niveaux correspondant aux critères de sécurité (disponibilité, confidentialité, intégrité, preuve, etc.) qu'il convient d'assurer à un élément essentiel.
CNIL	:	commission nationale de l'informatique et des libertés.
Commanditaire	:	alloue les budgets et les moyens humains permettant de répondre au besoin exprimé.
Commission d'homologation	:	instituée par l'AH, elle est chargée de fournir un avis motivé sur la capacité du SI à traiter les informations protégées au niveau de sécurité requis. La commission d'homologation prépare et conduit la démarche d'homologation du SI. La commission d'homologation du SI a pour mandat : - d'examiner le dossier d'homologation ; - de recueillir l'avis des experts en informatique et en SSI ; - de proposer à l'autorité d'homologation un avis motivé sur le niveau de sécurité atteint par le système et le niveau des risques résiduels quantifiés en termes de confidentialité, d'intégrité et de disponibilité en vue de l'emploi du SI. Principes et règles de fonctionnement : - le président de la commission d'homologation de sécurité fixe la liste des membres et des experts de la commission ; - la commission se réunit, autant que de besoin, sur convocation de son président afin de suivre l'état d'avancement du dossier d'homologation et des diverses actions lancées en vue de l'homologation du SI ; - lorsque le dossier d'homologation est finalisé, la commission d'homologation de sécurité se réunit et émet un avis qui peut éventuellement être assorti de réserves ; - le RSSI assure le secrétariat de la commission ; - les avis de la commission sont transmis à l'autorité d'homologation pour décision.
Contrôle de conformité	:	

		démarche qui consiste à s'assurer que le SI déployé dans l'environnement local s'exécute avec le niveau de sécurité requis par l'homologation de référence. Elle se concrétise par une décision de déploiement fondée sur une déclaration de conformité prononcée par l'autorité hiérarchique du site sur lequel le SI est déployé.
Directeur du projet	:	responsable de la conduite du projet, il a la maîtrise du budget, du calendrier et des performances, y compris des performances de sécurité.
Dossier d'homologation	:	ensemble de documents sur lequel s'appuie la commission d'homologation pour prononcer son avis.
Expression des besoins et identification des objectifs de sécurité (EBIOS)	:	méthode d'appréciation des risques SSI, et aussi véritable outil d'assistance à la maîtrise d'ouvrage (définition d'un périmètre d'étude, expression de besoins, responsabilisation des acteurs, etc.). Associée aux critères communs et aux avancées dans le domaine de la gestion de la sécurité de l'information (par exemple la norme ISO 27002), EBIOS devient aussi une méthode de traitement des risques SSI. Elle permet de rationaliser des objectifs et des exigences de sécurité en fonction de risques identifiés et éventuellement retenus.
Environnement de sécurité	:	conformément aux pratiques internationales en vigueur [organisation du traité de l'Atlantique Nord (OTAN) et union européenne (UE)], on distingue les trois niveaux d'environnement suivants : - l'environnement de sécurité physique global (GSE) désigne l'environnement physique général dans lequel est situé le système ; - l'environnement de sécurité local (LSE), inclus dans le GSE, recouvre l'environnement de sécurité physique, du personnel, documentaire et procédurale relevant du domaine de l'autorité d'homologation ; - l'environnement de sécurité électronique (ESE), inclus dans le LSE, désigne les mesures techniques de sécurité mises en place au niveau du système.
Exigences de sécurité	:	spécification fonctionnelle ou d'assurance sur le SI ou sur l'environnement de celui-ci, portant sur les mécanismes de sécurité à mettre en œuvre et couvrant un ou plusieurs objectifs de sécurité.
Expert SSI	:	personne qui apporte le soutien technique requis (conseil, conception de sécurité, évaluation, etc.) en fonction de la phase du cycle de vie du SI, au profit des autres acteurs. Il émet un avis technique sur la validité des mesures de protection employées. Ce rôle est habituellement tenu par plusieurs acteurs.
Fiche d'expression rationnelle des objectifs de sécurité des systèmes d'information (FEROS)	:	document formalisant tous les éléments SSI nécessaires à l'acceptation de la mise en œuvre d'un système par une autorité. Il présente donc non seulement tous les objectifs de sécurité du système étudié et les risques résiduels, mais aussi la démarche et l'argumentation qui a permis de les identifier. La méthode EBIOS facilite sa réalisation.
Gestion des risques	:	activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque. La gestion du risque inclut typiquement l'appréciation du risque, le traitement du risque, l'acceptation du risque et la communication relative au risque.
Fonctionnaire de sécurité des systèmes d'information (FSSI)	:	le FSSI est chargé de s'assurer de la bonne exécution des directives et orientations ministérielles et interministérielles ainsi que de la coordination et de la cohérence des actions menées dans le ministère. À ce titre, il veille à la conformité des démarches d'homologation de sécurité du SI vis-à-vis de la politique de sécurité des SI du ministère. Le FSSI est membre de droit de la commission d'homologation et peut se faire représenter aux différentes commissions d'homologation de sécurité.
HFCDS	:	haut fonctionnaire correspondant de défense et de sécurité.
Homologation de sécurité	:	déclaration par l'autorité d'homologation, au vu du dossier d'homologation, que le système d'information considéré est apte à traiter des informations d'un niveau de classification donné conformément aux objectifs de sécurité visés, et que les risques de sécurité résiduels sont acceptés et maîtrisés. L'homologation de sécurité reste valide tant que le SI opère dans les conditions approuvées par l'autorité d'homologation.
	:	

Homologation sous contrainte d'homologations		il s'agit d'une approche de l'homologation où un méta système est partitionné en systèmes qui font l'objet chacun de leur propre stratégie d'homologation. Certains de ces systèmes apportent des services de sécurité (et des vulnérabilités) à d'autres composants. Il découle de cette approche modulaire de l'homologation des contraintes « inter stratégies d'homologation ». L'approche permet de stabiliser la réduction des risques au fur et à mesure de la mise en exploitation des différents modules et donc une certaine indépendance de la gestion des systèmes dans le méta système.
Information	:	tout renseignement ou tout élément de connaissance susceptible d'être représenté sous une forme adaptée à une communication, à un enregistrement ou à un traitement.
Information ou support classifié	:	procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier présentant un caractère de secret de la défense nationale (article 413-9. du code pénal).
Information sensible	:	désigne une information dont la confidentialité, la disponibilité et l'intégrité ne procèdent pas du secret de la défense nationale tel que défini par les articles 413-9. à 413-12. du code pénal. Une information sensible est néanmoins protégée par des dispositions telles que l'obligation de discrétion professionnelle, le secret professionnel, les textes sur les données à caractère personnel et les obligations contractuelles.
M@rgeride	:	méthode d'analyse rapide et de gestion évolutive des risques dérivée d'EBIOS. Elle permet d'étendre EBIOS à la gestion des risques, à l'aide d'un outil simple et aisément partageable, pouvant « auto-porter » l'ensemble de la démarche SSI d'un projet ou d'un SI, pour aboutir à la mise en place d'une gestion dynamique des risques, éventuellement complétée par la mise en place d'un système de management de la sécurité de l'information (SMSI).
Menace	:	attaque possible d'un élément menaçant sur des biens. Cela regroupe à la fois le scénario et les moyens mis en œuvre.
Mesure de sécurité	:	moyen destiné à améliorer la sécurité, spécifié par une exigence de sécurité et à mettre en oeuvre pour la satisfaire. Il peut s'agir de mesures de prévision ou de préparation, de dissuasion, de protection, de détection, de confinement, de « lutte », de récupération, de restauration, de compensation, etc.
Objectif de sécurité	:	expression de l'intention de contrer des menaces ou des risques identifiés (selon le contexte) ou de satisfaire à des politiques de sécurité organisationnelles et à des hypothèses ; un objectif peut porter sur le système cible, sur son environnement de développement ou sur son environnement opérationnel.
Outil métier de la SSI	:	outil de suivi et de conduite des homologations.
Procédure d'exploitation de sécurité (PES)	:	document qui détaille la procédure à suivre pour que le système fonctionne en toute sécurité.
Politique de sécurité du système (PSS)	:	ensemble, formalisé dans un document applicable, des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection du (des) système(s) d'information de l'organisme.
Politique de sécurité du système d'information (PSSI)	:	politique qui établie les principes et les exigences, techniques et organisationnels, de sécurité du système. Elle est approuvée par l'AH.
Politique de sécurité technique (PST)	:	ensemble de règles techniques qui découlent de la PSS.
Responsable SSI	:	l'IM 900 (1) distingue le RSSI projet et le RSSI aval et en fixe les responsabilités. Le RSSI-P est chargé de piloter la démarche d'intégration de la SSI durant la phase projet ou programme, jusqu'à l'homologation initiale incluse, qu'il est chargé d'instruire. Le RSSI-A est chargé d'assurer le suivi SSI du système en service. À ce titre, il assure le secrétariat de la commission d'homologation et du GT SSI lorsqu'ils sont constitués.
Révision d'homologation	:	la révision d'une homologation du SI est nécessaire dans les cas suivants : - terme échu de l'homologation du SI ; - modification des objectifs de sécurité ;

- modification des conditions de sécurité du système ;

- modification de l'environnement (modification de la force des mécanismes de sécurité du réseau support, interconnexion, etc.) ;

- révision de l'homologation du réseau support et des éventuelles homologations contraignant la présente homologation (cas des homologations sous contrainte d'homologation) ;

- découverte de faille majeure dans le système sans correctif connu ;

- incident majeur (atteinte à la confidentialité, à l'intégrité ou à la disponibilité des informations traitées ou des informations nécessaires au fonctionnement du système lui-même) ;

- modification majeure du SI ;

- résultats non satisfaisants d'une inspection et d'un audit de sécurité.

En préparation à chaque révision, le dossier d'homologation est consolidé par les éventuelles analyses de vulnérabilités, rapports d'audit complémentaires ou autres investigations de toute sorte. Les membres de droit sont alertés des résultats. Le dossier est éventuellement transmis aux acteurs ne disposant pas d'un accès à l'application métier de la SSI. Pour un renouvellement d'homologation arrivant en fin de période de validité, un audit de sécurité sera mené (selon le SI). Les dates et les modalités sont alors arrêtées par l'autorité d'homologation en liaison avec l'organisme support.

Risque : combinaison d'une menace et des pertes qu'elle peut engendrer, c'est-à-dire de l'opportunité de l'exploitation d'une ou plusieurs vulnérabilités d'une ou plusieurs entités par un élément menaçant employant une méthode d'attaque avec l'impact sur les éléments essentiels et sur l'organisme.

Risque résiduel : risque subsistant après la démarche de gestion des risques.

Sécurité d'un système d'information : état de protection, face aux risques identifiés, qui résulte de l'ensemble des mesures générales et particulières prises pour assurer :

- la disponibilité, c'est-à-dire l'aptitude du système à remplir une fonction dans des conditions définies d'horaires, de délais et de performances ;

- l'intégrité (2) du système et de l'information traitée qui garantit que ceux-ci ne sont modifiés que par une action volontaire et légitime. Lorsque l'information est échangée, l'intégrité s'étend à l'authentification du message, c'est-à-dire à la garantie de son origine et de sa destination ;

- la confidentialité, c'est-à-dire le caractère réservé d'une information dont l'accès est limité aux seules personnes admises à la connaître pour les besoins du service.

SHEM ou SHéM : structure d'hébergement mutualisé.

Stratégie d'homologation : ce document, partie intégrante du dossier d'homologation, précise :

- la cible de l'homologation ;

- les étapes de la démarche d'homologation ;

- les actions à réaliser, les livrables attendus et les acteurs concernés ;

- la liste des documents constituant le dossier d'homologation, les acteurs concernés par leur rédaction et les échéances afférentes.

Validée et promulguée par l'AH, la stratégie d'homologation de sécurité a valeur d'ordre pour tous les acteurs impliqués dans la mise en œuvre du SI.

Système d'information (SI)	:	le système d'information est constitué de l'ensemble organisé des ressources (personnels, matériels, logiciels) permettant de collecter, stocker, traiter et communiquer les informations. Le système d'information appuie les activités de l'organisation et contribue à l'atteinte des objectifs.
Système d'information sensible	:	système d'information qui supporte une ou plusieurs applications sensibles, ou qui comporte une ou plusieurs informations sensibles, ou qui offre un service et dont la perte de sécurité porterait préjudice à la continuité du fonctionnement des services de l'État et de l'exercice du pouvoir, en situation normale comme en situation de crise. Il se classe dans l'une des 3 catégories suivantes [au sens du guide interministériel n° 730/SCSSI du 13 janvier 1997 (1) sur les systèmes d'information et applications sensibles] : - 1re catégorie : systèmes d'information et applications sur lesquels une atteinte à la disponibilité, à l'intégrité ou à la confidentialité peut entraîner la neutralisation d'une fonction majeure dans le fonctionnement des services de l'État et l'exercice du pouvoir (fonction rendue totalement inexploitable pendant une durée inacceptable, avec des conséquences graves ou très graves) ; - 2e catégorie : systèmes d'information et applications sur lesquels une atteinte à la disponibilité, à l'intégrité ou à la confidentialité peut entraîner une dégradation du fonctionnement des services de l'État et de l'exercice du pouvoir (fonctionnement fortement et durablement perturbé, avec des conséquences importantes) ; - 3e catégorie : systèmes d'information et applications sur lesquels une atteinte à la disponibilité, à l'intégrité ou à la confidentialité peut entraîner une gêne dans le fonctionnement des services de l'État et l'exercice du pouvoir (fonctionnement faiblement perturbé, avec des conséquences limitées).
Utilisateur du système	:	l'utilisateur du système est responsable des informations et des équipements qu'il exploite ou traite. Il doit se conformer aux procédures d'exploitation de sécurité. L'utilisateur fait remonter tout incident de sécurité à l'OSSI local auquel il est rattaché.

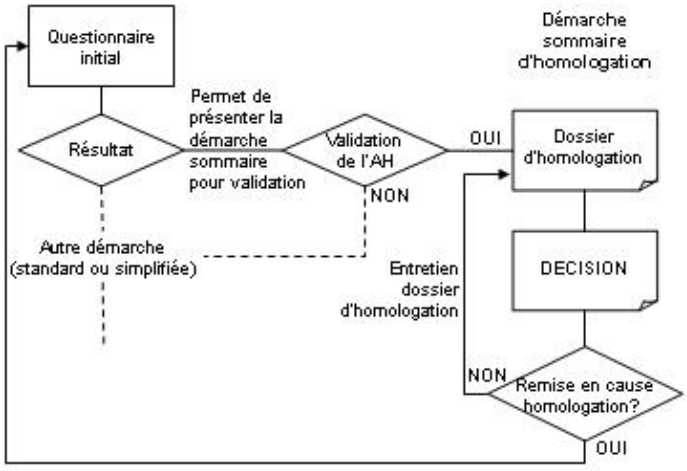
---

(1) n.i. BO.

(2) Le besoin de sécurité en preuves de qualité opposable, rendu possible par la signature électronique et l'authentification forte est couvert par le concept intégrité.

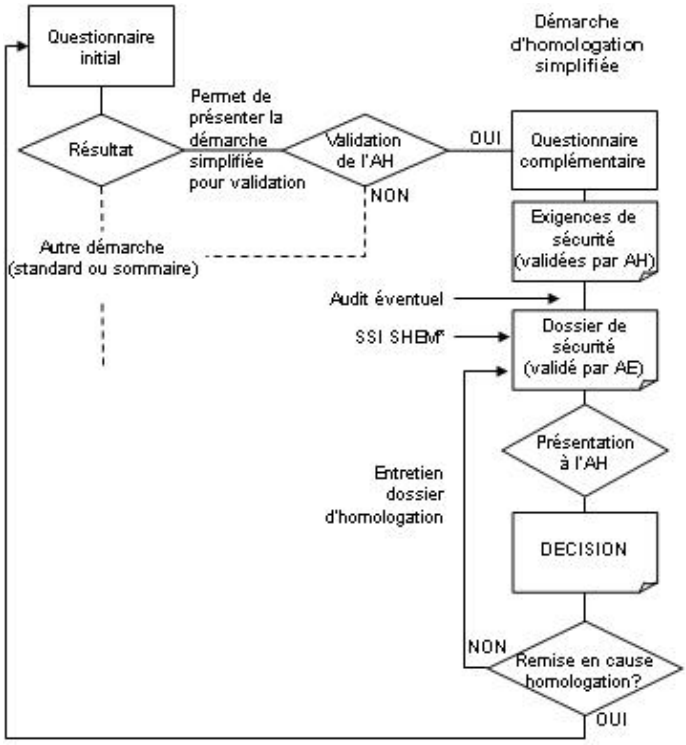
ANNEXE II.

SCHÉMA DE PRINCIPE DE LA DÉMARCHE SOMMAIRE D'HOMOLOGATION.



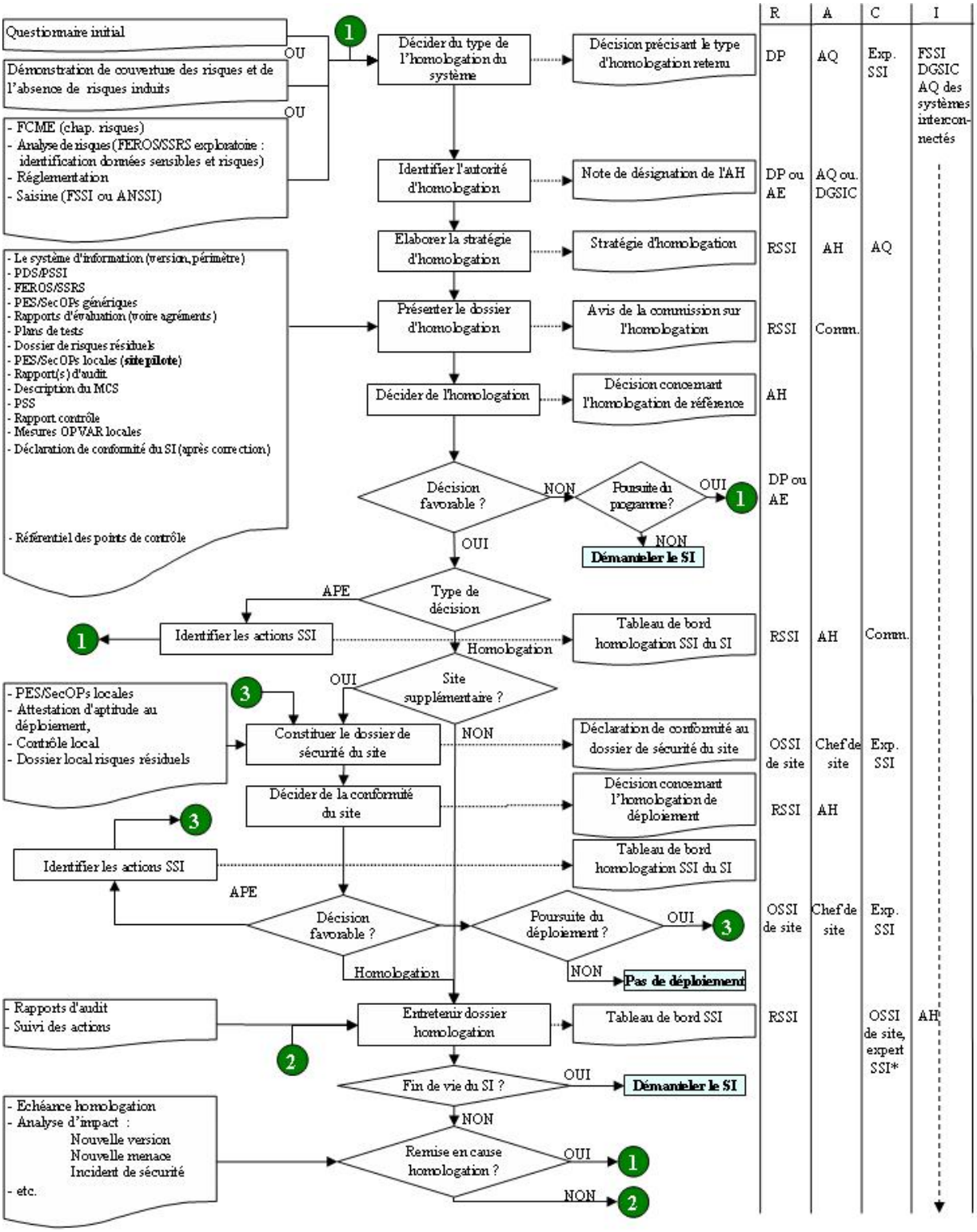
ANNEXE III.

SCHÉMA DE PRINCIPE DE LA DÉMARCHE D'HOMOLOGATION SIMPLIFIÉE.



ANNEXE IV.

SCHÉMA DE PRINCIPE DE LA DÉMARCHE D'HOMOLOGATION STANDARD.



ANNEXE V.

COMPOSITION DU DOSSIER D'HOMOLOGATION.

DOSSIER D'HOMOLOGATION : DÉMARCHE SOMMAIRE.
Validés par l'AH : - questionnaire ou justificatif équivalent et décision relative à la démarche ; - décision d'homologation.

DOSSIER D'HOMOLOGATION : DÉMARCHE SIMPLIFIÉE.
Validés par l'AH : - questionnaire ou justificatif équivalent et décision relative à la démarche ; - décision d'homologation ; - exigences de sécurité.
Dossier simplifié de sécurité validé par l'AE : - PDS ; - PES ; - fiche de synthèse des risques résiduels.
Certificat(s) de conformité (si nécessaire).

Ces pièces peuvent constituer un seul et même document.

DOSSIER D'HOMOLOGATION : DÉMARCHE STANDARD.
Décision relative à la démarche.
Stratégie d'homologation.
Saisines éventuelles.
FEROS.
Politique de sécurité du SI (PSS).
Plan de sécurité (PDS).
Procédure d'exploitation de sécurité (PES).
Plan de continuité/reprise informatique (PCI/PRI) (si nécessaire).
Rapports d'audit et tests de sécurité.
Décisions de labellisation (si existantes).
Référentiel des points de contrôle (plan de test).
Fiche de synthèse des risques résiduels.
Certificat(s) de conformité (si nécessaire).

ANNEXE VI.

PLAN TYPE D'UNE STRATÉGIE D'HOMOLOGATION.

1. PRÉSENTATION DU SYSTÈME D'INFORMATION.

1.1. **Généralités.**

Ce point contient une présentation générale du système.

1.2. **Architecture.**

Ce point contient l'architecture générale du système.

L'architecture doit mettre en évidence les interconnexions éventuelles tant internes qu'externes au ministère ainsi que les SI avec lesquels il échange des données.

Il faut préciser les équipements devant faire l'objet d'une attention particulière (exemple : passerelle, chiffreur, etc.).

1.3. **Conditions générales d'emploi.**

Ce point contient les conditions générales d'emploi du système en mode de fonctionnement dégradé et normal. Il s'agit d'expliquer comment le système doit répondre au besoin de l'autorité d'emploi en situation de crise.

1.4. **Fonctions critiques du système.**

Si le système est identifié comme critique (voir directive sur les systèmes critiques), ce point recense l'ensemble des fonctions du système jugées critiques.

1.5. **Maintien en conditions opérationnel et de sécurité.**

Ce point décrit succinctement l'organisation mise en œuvre pour assurer le soutien du SI et particulièrement la prise en compte de la SSI dans le soutien du système (maintenance préventive, corrective des logiciels et matériels, que ce soit vis-à-vis des pannes ou des vulnérabilités identifiées). Il peut faire référence à la directive de soutien du système et au document traitant de son maintien en conditions de sécurité.

1.6. **Périmètre d'homologation.**

Ce point doit décrire précisément ce qui fait partie du périmètre d'homologation (cf. point 4.6. de la présente directive).

1.7. **Objectif de sécurité.**

Ce point précise si une analyse de sécurité a été effectuée ainsi que la méthode employée et si les objectifs de sécurité ont été traduits dans la FEROS.

1.8. **Qualification/évaluations et audits.**

Ce point cite les différentes entités responsables de la qualification de tout ou partie du système, des évaluations ou des audits.

Il permet de préciser également les besoins en audit, en tests d'intrusion ainsi que leurs fréquences et en évaluations éventuelles des outils de sécurité, etc.

2. COMMISSION D'HOMOLOGATION.

La composition de la commission est décrite dans le tableau en appendice VI.B.

2.1. **Membres permanents (1).**

Le président peut faire appel à toute personne qualifiée en raison de sa compétence ou de ses fonctions pour être membre à titre permanent.

2.2. **Membres associés (1).**

Le président peut faire appel à toute personne qualifiée en raison de sa compétence ou de ses fonctions pour être entendue à titre d'expert ainsi qu'aux autorités concernées par les questions inscrites à l'ordre du jour.

Le FSSI et l'AQ peuvent participer à toute commission d'homologation.

3. DÉMARCHE D'HOMOLOGATION.

La démarche d'homologation est maintenue tout le long du cycle de vie du système d'information et prend fin après le retrait de service du SI.

La gestion des homologations est outillée par l'application métier de la SSI. À ce titre, l'ensemble des informations concourant à l'homologation du SI est centralisé dans l'application, dans la limite du niveau de protection apporté par l'application. Le RSSI est responsable de la mise à jour des données. Néanmoins, les acteurs SSI impliqués apporteront directement dans l'application les compléments d'information nécessaires à la compréhension globale du niveau de sécurité du SI.

3.1. **Planification.**

Le calendrier prévisionnel de la démarche d'homologation est spécifié en appendice VI.C.

3.2. **Durée de validité de l'homologation.**

L'homologation de NOM_DU_SI peut être prononcée pour une durée maximale de X ans.

3.3. **Processus de suivi après l'homologation initiale du système d'information.**

La commission d'homologation se réunit périodiquement sur convocation de l'autorité d'homologation pour statuer sur le maintien de l'homologation.

4. DOCUMENTATION DE RÉFÉRENCE.

Citer dans ce point les documents de sécurité constituant le dossier d'homologation.

APPENDICE VI.A.

DOCUMENTATION DE RÉFÉRENCE.

DOCUMENTATION DE RÉFÉRENCE.

APPENDICE VI.B.

COMMISSION D'HOMOLOGATION.

COMMISSION D'HOMOLOGATION.

OBLIGATOIRE	NOM ou ORGANISATION
Autorité d'homologation et président de la commission	
Responsable de sécurité des systèmes d'information projet (RSSI-P) [ou responsable de sécurité des systèmes d'information aval (RSSI-A) pour une ré-homologation]	
Directeur de projet/programme	
Représentant de l'autorité d'emploi	

INVITÉ	NOM ou ORGANISATION
FSSI	
AQ	
Officier de projet/programme	
Représentant du bureau central SSI de la direction de projet/programme	
Commanditaire*	
…	

SI NÉCESSAIRE	NOM ou ORGANISATION
RSSI du réseau support sur lequel le SI est implémenté	
Autorité(s) d'exploitation	
Représentant de l'opérateur du réseau support	
Responsable du ou des audits de sécurité ou VASSI	
Responsable de la maîtrise d'œuvre du projet	
Responsable de l'hébergement de l'application	
Expert SSI	
…	

APPENDICE VI.C.

PLANIFICATION DE LA DÉMARCHE D'HOMOLOGATION.

PLANIFICATION DE LA DÉMARCHE D'HOMOLOGATION.

(1) Liste non exhaustive.

ANNEXE VII.

DÉCISION D'HOMOLOGATION.

DÉCISION D'HOMOLOGATION.

Le ***FONCTION_DU_PRESIDENT***, président de la commission d'homologation réunie le ***JJ/MM/AAAA***, dont la composition figure en appendice I.A., agissant en tant :

qu'autorité d'homologation désignée par ***REFERENCE_ET_DATE_DU_DOCUMENT***

DECIDE

que le système d'information ***NOM_DU_SI*** situé à ***IMPLANTATION GEOGRAPHIQUE PRECISE*** est homologué au niveau ***NIVEAU_RETENU*** dans la configuration présentée en appendice VI.B. ;

que ce système est la plate-forme de référence pour les installations futures du système ***NOM_DU_SI***

La présente décision d'homologation est valable à compter du ***JJ/MM/AAAA*** jusqu'au ***JJ/MM/AAAA***

Toute modification du système et/ou de son environnement annule la présente décision.

ATTACHE ET SIGNATURE

ANNEXE VIII.

AUTORISATION PROVISOIRE D'EXPLOITATION.

AUTORISATION PROVISOIRE D'EXPLOITATION.

Le ***FONCTION_DU_PRESIDENT***, président de la commission d'homologation réunie le ***JJ/MM/AAAA***, dont la composition figure en appendice I.A., agissant en tant :

qu'autorité d'homologation désignée par ***REFERENCE_ET_DATE_DU_DOCUMENT***

CONSIDERANT

- ***soit un aspect opérationnel ;***
- ***soit un risque accepté pour une durée limitée.***

DECIDE

que le système d'information ***NOM_DU_SI*** situé à ***IMPLANTATION GEOGRAPHIQUE PRECISE*** est homologué au niveau ***NIVEAU_RETENU*** dans la configuration présentée en appendice VI.B. ;

et PRONONCE

une autorisation provisoire d'exploitation du système d'information ***NOM_DU_SI*** assortie de la condition suivante :

- ***soit de retrait du service à l'issue de l'APE ;***
- ***soit de correction des faits constatés en vue d'une homologation en bonne et due forme et précisées en annexe et dont les opérations seront conduites par DESIGNATION_DE_L'AUTORITE, directeur du système.***

La présente décision d'autorisation provisoire d'exploitation est valable[1] à compter du ***JJ/MM/AAAA*** jusqu'au ***JJ/MM/AAAA***

Toute modification du système et / ou de son environnement annule la présente décision.

ATTACHE ET SIGNATURE

[1] : durée limitée à 6 mois, renouvelable une fois.

ANNEXE IX.

REFUS D'HOMOLOGATION.

REFUS D'HOMOLOGATION.

Le ***FONCTION_DU_PRESIDENT***, président de la commission d'homologation réunie le ***JJ/MM/AAAA***, dont la composition figure en appendice I.A., agissant en tant :

qu'autorité d'homologation désignée par ***REFERENCE_ET_DATE_DU_DOCUMENT***

DECIDE

que le système d'information ***NOM_DU_SI*** situé à ***IMPLANTATION GEOGRAPHIQUE PRECISE*** n'est pas homologué pour la (les) raison(s) précisée(s) en appendice VI.B.

ATTACHE ET SIGNATURE

ANNEXE X.

DÉCLARATION D'APTITUDE.

DÉCLARATION D'APTITUDE.

Le ***FONCTION_DU_PRESIDENT***, président de la commission d'homologation réunie le ***JJ/MM/AAAA***, dont la composition figure en appendice I.A., agissant en tant qu'autorité d'homologation désignée par ***REFERENCE_ET_DATE_DU_DOCUMENT***

DECLARE

que le système d'information ***NOM_DU_SI*** situé à ***IMPLANTATION GEOGRAPHIQUE PRECISE*** est apte à être exploité au niveau ***NIVEAU_RETENU*** dans la configuration présentée en appendice VI.B. ;

que ce système est la plate-forme de référence pour les installations futures du système ***NOM_DU_SI***

La présente déclaration d'aptitude est valable à compter du ***JJ/MM/AAAA***

Toute modification du système et / ou de son environnement annule la présente décision.

ATTACHE ET SIGNATURE

ANNEXE XI.

CERTIFICAT DE CONFORMITÉ.

CERTIFICAT DE CONFORMITÉ.

Le ***AUTORITE_HIERARCHIQUE_DU_SITE***, responsable du déploiement du ***NOM_DU_SI*** sur le site de ***IMPLANTATION GEOGRAPHIQUE PRECISE***

CERTIFIE

que les mesures locales de sécurité pour le déploiement du ***NOM_DU_SI*** sont conformes à celles décrites dans le dossier de sécurité de référence ***REFERENCE DU DOCUMENT***.

La situation des mesures locales de sécurité par rapport aux procédures d'exploitation de sécurité du système ***NOM_DU_SI*** est fournie en appendice VI.B.

Le présent certificat de conformité est valable à compter du ***JJ/MM/AAAA*** jusqu'au ***JJ/MM/AAAA*** [1]

ATTACHE ET SIGNATURE

[1] : durée de l'homologation de référence.