MINISTÈRE
DE L'AGRICULTURE
ET DE LA SOUVERAINETÉ
ALIMENTAIRE
Liberté
Égalité
Fraternité

Ordre de méthode

Secrétariat général **Service du numérique** **Sous-direction de la stratégie, du pilotage et des ressources** **Bureau de la sécurité des systèmes d'information**	**Instruction technique** **SG/SNUM/SDSPR/2023-576** **14/09/2023**

Date de mise en application : Immédiate
Diffusion : Tout public

Cette instruction abroge :
SG/SM/SDSI/MSSI/N2012-1403 du 28/03/2012 : Homologation de sécurité des systèmes d'information
CAB/MD/N2012-0004 du 28/03/2012 : Homologation de sécurité des systèmes d'information
Cette instruction ne modifie aucune instruction.
Nombre d'annexes : 0

Objet : Organisation de l'homologation de sécurité des systèmes d'information au MASA

Destinataires d'exécution
Administration centrale Services déconcentrés

Résumé : Cette note de service précise la procédure d'homologation des systèmes d'information du MASA. Elle désigne les autorités d'homologation relativement à un système d'information à homologuer, décrit la procédure d'homologation au MASA et précise les conséquences de cette homologation.

Textes de référence :
- Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.
- Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'Ordonnance 2005-1516 du 8 décembre 2005 relatif à la sécurité des informations échangées par voie électronique.

- Décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique
- Décret n° 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics
- Arrêté du 26 octobre 2022 portant approbation de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI sur l'organisation de la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics
- Décret n° 2023-304 du 22 avril 2023 modifiant le décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique

CONTEXTE

L'homologation est une nécessité associée à la mise en service opérationnelle de tout système d'information au sein de l'Etat. Elle doit être régulièrement réexaminée, afin de prendre les mesures que peuvent imposer les évolutions du système, de ses composants, de son emploi, du contexte humain ou organisationnel, ou encore bien sûr de la menace.

Afin de permettre d'identifier, d'atteindre puis de maintenir un niveau de risque de sécurité acceptable pour un système d'information compte-tenu du besoin de protection requis, une démarche d'homologation globale doit être conduite. Ainsi, s'appuyant sur une gestion globale des risques de sécurité concernant l'ensemble du système d'information, l'homologation de sécurité inclut dans son périmètre les aspects techniques et organisationnels.

L'autorité d'homologation assume la responsabilité afférente à la décision d'homologation notamment pour accepter les risques résiduels. **Cette décision d'homologation est l'engagement par lequel l'autorité d'homologation atteste, au nom de l'autorité administrative, que le projet a bien pris en compte les contraintes opérationnelles de sécurité établies au départ, que les exigences de sécurité sont bien déterminées et satisfaites, que les risques résiduels sont maîtrisés et acceptés.**

Note importante : le présent document ne vise que l'administration centrale et les services déconcentrés du MASA. Les établissements publics doivent organiser leur propre procédure d'homologation.

1. ORGANISATION DE L'HOMOLOGATION DES SI AU MASA

1.1 Instances

1.1.1 L'autorité d'homologation

Le décret n° 2019-1088 du 25 octobre 2019 modifié relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique détaillant la mise en œuvre de la nouvelle gouvernance de la sécurité numérique de l'État stipule en son article 4-2 :

> *« L'autorité qualifiée en sécurité des systèmes d'information [AQSSI] est responsable de la sécurité numérique des systèmes d'information et de communication relevant de ses attributions. A ce titre, elle définit la politique de sécurité numérique qui leur est applicable et contrôle son application au travers notamment de l'homologation de ces systèmes d'information prévue à l'article 4-3. Elle peut déléguer cette fonction d'homologation à des autorités d'homologation qu'elle désigne. »*

Par conséquent, **les AQSSI sont en charge de l'homologation de leurs systèmes d'information au sein de chacune de leurs structures**. Pour le MASA, les AQSSI sont les directeurs de l'administration centrale et des services déconcentrés.

L'AQSSI est assisté dans ce rôle par son Conseiller à la sécurité numérique (CSN). Le CSN est désigné dans chaque structure par l'AQSSI.

1.1.2 L'analyse de sécurité

Tout système d'information objet d'une homologation fait l'objet d'une étude complète de sécurité. Cette étude est réalisée par le Bureau de la sécurité des systèmes d'information du Service du numérique (SNum/SPR/BSSI), qui émet un avis consultatif sur le caractère homologable ou pas de cette application.

1.1.3 La commission d'homologation

La commission d'homologation assiste l'AQSSI pour prononcer l'homologation d'un système d'information. Elle est présidée par le chef du Service du numérique. Son secrétariat est assuré par le BSSI.

Elle est composée :

- du Chef du Service du numérique, en charge de la présidence de la commission,
- de l'AQSSI du service en charge de la maîtrise d'ouvrage du SI concerné par l'homologation,
- de son CSN,
- du représentant de la structure en charge opérationnellement de la maîtrise d'ouvrage de l'application,
- de la Haute-fonctionnaire de défense et de sécurité adjointe, cheffe du Service de défense et de sécurité,
- de la Sous-directrice de la stratégie, du pilotage et des ressources du SNum,
- du FSSI,
- du Chef du Bureau de la sécurité des systèmes d'information du SNum.

La commission peut se faire assister de tout expert dont l'avis est jugé nécessaire par le président de la commission, l'AQSSI ou bien un autre membre de la commission d'homologation.

1.2 Procédure d'homologation

1.2.1 Saisine

Deux voies de saisines existent pour l'homologation d'un système d'information du MASA.

1.2.1.1 Saisine directe par l'AQSSI

Lorsqu'un AQSSI doit prononcer l'homologation d'un système d'information de son périmètre, **préalable à toute mise en service opérationnelle d'un SI**, il saisit le Service du numérique pour obtenir l'ensemble de documents nommé « Dossier de sécurité en vue de l'homologation d'un système d'information ». Cette saisine est adressée à l'adresse de messagerie : liste-homologation-SI-sg@agriculture.gouv.fr.

Après réalisation de l'analyse de sécurité, le BSSI se prononce sur le caractère homologable ou non du système, notamment au regard du parcours de ce système dans la méthode permettant la sécurisation des SI au MASA nommée méthode ISP (intégration de la sécurité dans les projets) :

- si le BSSI considère que le système ne répond pas aux critères de l'homologation, par exemple parce qu'il n'a pas terminé son parcours de sécurité, un avis motivé en ce sens est envoyé par le chef du SNum ou son représentant à l'AQSSI en vue de repousser la décision d'homologation ;
- si le BSSI considère que le SI a suivi avec succès le parcours de sécurité de la méthode ISP, il transmet pour validation au chef du SNum le « Dossier de sécurité en vue de l'homologation d'un système d'Information », avec son avis relatif à l'homologation du système d'information.

Le chef du SNum ou son représentant, après validation, transmet à l'AQSSI ainsi qu'à l'ensemble des membres de la commission d'homologation le « Dossier de sécurité en vue de l'homologation d'un système d'information ».

1.2.1.2 Auto-saisine du BSSI

Dès lors qu'un système d'information est arrivé à la fin du parcours de sécurité de la méthode ISP, méthode systématiquement utilisée au MASA pour l'ensemble des systèmes d'information, le BSSI peut s'autosaisir relativement au caractère homologable d'un système. Ainsi, si le SI a suivi avec succès le

parcours de sécurité de la méthode ISP, le BSSI peut proposer l'homologation du système d'information et il transmet pour validation au chef du SNum le « Dossier de sécurité en vue de l'homologation d'un système d'Information ».

Le chef du SNum ou son représentant, après validation, transmet alors à l'AQSSI ainsi qu'à l'ensemble des membres de la commission d'homologation le « Dossier de sécurité en vue de l'homologation d'un système d'information ».

1.2.1.3 Contenu du « Dossier de sécurité en vue de l'homologation d'un système d'information »

Ce dossier contient l'ensemble des éléments permettant de se prononcer sur l'adéquation du niveau de sécurité d'un système d'information relativement à sa sensibilité préalablement évaluée. Il comprend notamment :

1) la pré-étude de sécurité permettant de déterminer le niveau de sensibilité du SI en Disponibilité, Intégrité, Confidentialité et en Preuve (DICP) ;

2) une fiche de synthèse de sécurité listant :
- l'ensemble des actions de sécurité mises en œuvre,
- l'ensemble des tests de sécurité ou audits réalisés ainsi que leurs résultats communicables,
- l'ensemble des éventuelles corrections réalisées,
- l'ensemble des éventuels risques ou vulnérabilités résiduels ainsi que leurs impacts,
- l'avis motivé du BSSI sur le caractère homologable (éventuellement avec réserves) ou pas de l'application ;

3) une proposition de décision d'homologation du système (si l'avis du BSSI est positif) reprenant en synthèse les éléments précédents.

S'il le juge nécessaire, le BSSI peut adjoindre au dossier tout document propre à informer l'AQSSI et les membres de la commission d'homologation sur le niveau de sécurité du système d'information.

1.2.2 Prononcé de l'homologation par l'AQSSI

1.2.2.1 Prononcé direct de l'homologation

Après transmission par le SNum du « Dossier de sécurité en vue de l'homologation d'un système d'information » à l'AQSSI et aux membres de la commission d'homologation, ceux-ci ont un mois pour faire parvenir à l'AQSSI ainsi qu'au SNum (adresse de messagerie SNum : liste-homologation-SI-sg@agriculture.gouv.fr) leurs commentaires, oppositions ou observations, en précisant si ceux-ci sont de nature à remettre en cause l'avis du BSSI.

Si aucun membre de la Commission d'homologation ne fait part de commentaires, oppositions ou observations de nature à remettre en cause l'avis du BSSI dans un délai d'un mois, l'AQSSI peut signer la décision d'homologation transmise dans le « Dossier de sécurité en vue de l'homologation d'un système d'information ». Après signature, l'AQSSI transmet la décision signée au BSSI, qui la communique pour information à l'ensemble des membres de la commission d'homologation ; la décision est publiée selon les modalités prévues au chapitre 2 de ce document.

Si l'AQSSI ou un membre de la commission d'homologation a des commentaires, oppositions ou observations de nature à remettre en cause l'avis du BSSI, la commission d'homologation est réunie selon la procédure définie au 1.2.2.2.

1.2.2.2 Réunion de la commission d'homologation

En cas de commentaires, oppositions ou observations d'un des membres de la commission d'homologation (dont l'AQSSI lui-même) de nature à remettre en cause l'avis du BSSI, la commission d'homologation est réunie par le BSSI. Les débats tenus en commission d'homologation font l'objet d'un compte-rendu rédigé et diffusé par le BSSI.

En cas d'absence de consensus sur le caractère homologable de l'application, la décision finale revient à l'autorité d'homologation (AQSSI). La mise en service opérationnelle de l'application pourra toutefois être soumise à la mise en œuvre préalable de mesures d'isolation de l'application en vue de la préservation des autres SI sous responsabilité d'autres AQSSI ; ces mesures seront le cas échéant définies par le SNum.

Après réunion de la commission, l'AQSSI signe la décision d'homologation dans les conditions déterminées au 1.2.2.1 ou bien rejette l'homologation.

2. Conséquences de la décision d'homologation

2.1 Typologie des décisions

La décision d'homologation doit intervenir avant la mise en service opérationnelle du système.

Selon les résultats de la démarche d'homologation, l'autorité d'homologation peut prononcer :

- une homologation provisoire, assortie de réserves et d'un délai de mise en conformité des défauts de sécurité rencontrés ;
- une homologation, assortie le cas échéant de conditions, pour une durée déterminée de 3 à 5 ans. Dans le cas où persistent de nombreux risques résiduels, cette durée peut être réduite à 1 an ;
- un refus d'homologation, si les résultats du dossier de sécurité font apparaître des risques résiduels jugés inacceptables.

2.2 Mise en service

La mise en service du système ne peut intervenir qu'en cas de décision positive d'homologation.

Cependant, **lorsque l'urgence opérationnelle le requiert et de façon exceptionnelle**, il peut être procédé à une mise en service provisoire, sans attendre l'homologation du système, en tenant compte de l'avancement de la procédure d'homologation et des risques résiduels de sécurité. Dans ce cas, la mise en service définitive interviendra ultérieurement, lorsque l'homologation de sécurité aura été prononcée.

La mise en service provisoire d'un système d'information est décidée conjointement par l'Autorité d'homologation (AQSSI) et le chef du Service du numérique.

2.3 Communication des décisions d'homologation

Les décisions d'homologation sont rendues accessibles au sein du MASA par publication de la décision dans les mentions légales de l'application.

Dans le cas d'un téléservice, la décision est rendue accessible aux usagers qui doivent pouvoir la consulter au sein de ce téléservice.

2.4 Contrôle et renouvellement de l'homologation

L'autorité d'homologation (AQSSI), conjointement avec le chef du Service du numérique, fixent les conditions du maintien de l'homologation de sécurité au cours du cycle de vie du système d'information. Ils contrôlent régulièrement que le système fonctionne effectivement selon les conditions qu'ils ont approuvées, en particulier après des opérations de maintien en conditions opérationnelles et de maintien en conditions de sécurité. Les membres de la commission d'homologation sont informés par l'AQSSI de la réalisation de ces contrôles.

L'autorité d'homologation (AQSSI) est en charge de la demande de renouvellement de l'homologation lorsque l'application est toujours en fonctionnement à la fin de la date prévue pour la fin de la précédente homologation. La procédure de renouvellement est la même que celle de l'homologation initiale (cf. 1.2.1.1).

L'autorité d'homologation (AQSSI) ou le chef du Service du numérique examinent également le besoin de renouvellement de l'homologation avant le terme prévu notamment lorsque :

- les conditions d'exploitation du système ont été notablement modifiées ;
- des nouvelles fonctionnalités majeures ont été 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 ;
- les menaces sur le système ont évolué ou de nouvelles vulnérabilités ont été découvertes ;
- le système a fait l'objet d'un incident majeur de sécurité.

En cas de demande de renouvellement anticipé dans ce cadre, la procédure utilisée est aussi la même que celle de l'homologation initiale (cf 1.2.1.1).

La Secrétaire générale

Cécile BIGOT-DEKEYZER