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

Secrétariat général **Service du numérique** **78, rue de Varenne** **75349 PARIS 07 SP** **01 49 55 59 00 (PASTEL)** **Secrétariat général** **Service du numérique** **Sous-direction de la stratégie, du pilotage et des ressources** **Bureau de la sécurité des systèmes d'information** **mssi.sg@agriculture.gouv.fr**	**Instruction technique** **SG/SNUM/2026-57** **03/02/2026**

Date de mise en application : Immédiate
Diffusion : Tout public

Cette instruction n'abroge aucune instruction.
Cette instruction ne modifie aucune instruction.
Nombre d'annexes : 6

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

Destinataires d'exécution
Administration centrale Cabinet – Bureau du cabinet Services déconcentrés du MAASA

Résumé : cette note de service précise la procédure d'homologation des systèmes d'information du MAASA. Elle désigne les acteurs de l'homologation, décrit la procédure d'homologation au MAASA et précise les conséquences de cette homologation.

Textes de référence :
- Politique de sécurité des systèmes d'information de l'Etat, Premier ministre, N°5725/SG du 17 juillet 2014
- Politique de sécurité des systèmes d'information de l'Agriculture, Instruction technique, CAB/MD/2015-586, 09/07/2015
- 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° 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
- Arrêté du 31 juillet 2025 relatif aux dispenses d'homologation de sécurité des infrastructures et services logiciels informatiques qui composent le système d'information et de communication de l'Etat

CONTEXTE

L'homologation préalable est nécessaire à la mise en service opérationnelle de tout système d'information au sein de l'Etat.

Pour chaque système d'information considéré, la démarche d'homologation permet d'identifier, d'atteindre puis de maintenir un niveau de risque de sécurité. Pour ce faire, une analyse globale des risques est menée. Il est entendu que la démarche d'homologation prend en compte les aspects techniques et organisationnels.

La démarche d'homologation est avant tout destinée à faire connaître et faire comprendre aux responsables métiers les risques liés à l'exploitation d'un système d'information. Elle se conclut par une décision formelle prise par une autorité qualifiée en sécurité des systèmes d'information (AQSSI), soutenue par la constitution et l'analyse d'un dossier de sécurité par les services techniques appelé « fiche de sécurité » (cf. annexe 4).

Cette décision est l'engagement par lequel l'autorité d'homologation atteste, au nom de l'autorité administrative (la structure), 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 connus, maîtrisés et acceptés.

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

1. Instances et acteurs de l'homologation des SI au MAASA

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 MAASA, conformément à l'arrêté ministériel du 27 avril 2007, **les AQSSI sont le directeur de cabinet, la secrétaire générale, le président du CGAAER, et les directeurs de l'administration centrale et des services déconcentrés**.

L'AQSSI peut être assisté dans ce rôle par son Conseiller à la sécurité numérique (CSN) qu'il désigne au sein de son entité. Les décisions internes de désignation d'un CSN sont à porter à la connaissance du fonctionnaire de sécurité des systèmes d'information et du bureau de la sécurité des systèmes d'information (BSSI) au sein du service du numérique.

1.2 L'analyse de sécurité par le bureau de la sécurité des systèmes d'information (BSSI) du service du numérique

Cette analyse fait l'objet d'une pré-étude de sécurité dont le modèle est annexé au présent document (cf. annexe 1) puis d'un parcours de sécurité pouvant comprendre une analyse de risques EBIOS RM ainsi que différents types d'audits et tests d'intrusion.

Tout système d'information au sein du MAASA fait l'objet d'un parcours de sécurité. Celui-ci est réalisé par le BSSI du Service du numérique (SNum/SPR/BSSI), qui émet un avis consultatif sur le caractère homologable ou pas de cette application.

La pré-étude de sécurité est envoyée par le BSSI pour validation à l'entité en charge de la maitrise d'ouvrage (c'est-à-dire la structure en charge de mener le projet, projet sous la responsabilité de l'AQSSI). Cette pré-étude est validée par l'AQSSI ou, à défaut, son Conseiller à la sécurité du numérique (CSN).

1.3 Le rôle du FSSI

Le fonctionnaire de sécurité des systèmes d'information conseille et accompagne, au sein de son périmètre ministériel, sur les questions relatives à la sécurité numérique, y compris en matière d'homologation.

1.4 La commission d'homologation

La commission d'homologation assiste l'AQSSI pour prononcer l'homologation d'un système d'information.

Elle est composée :

- de l'AQSSI du service en charge de la maîtrise d'ouvrage du SI concerné par l'homologation, qui préside la commission d'homologation ;
- du Chef du Service du numérique ou son adjoint ;
- du conseiller à la sécurité du numérique (CSN) de la structure concernée ;
- du représentant de la structure en charge opérationnellement de la maîtrise d'ouvrage de l'application au sein de la structure ;
- de la Haute-fonctionnaire de défense et de sécurité adjointe, cheffe du Service de défense et de sécurité ;
- du Fonctionnaire de sécurité des systèmes d'information (FSSI) ;
- du Délégué à la protection des données (« Data Privacy Officer » - DPO) ;
- du Sous-Directeur de la stratégie, du pilotage et des ressources du SNum ;
- du Chef du Bureau de la sécurité des systèmes d'information du SNum.

La commission peut se faire assister de tout expert technique dont l'avis est jugé nécessaire par tout membre de la commission d'homologation et sous réserve de validation par le président de la commission.

Le secrétariat de la commission est assuré par le BSSI. Chaque commission donne lieu à un relevé de décision signé par l'AQSSI (cf. annexe 5)

2. Procédure d'homologation

La méthode d'intégration de la sécurité dans les projets (appelée « ISP ») vise à assurer un parcours de sécurité à tout projet informatique, produit informatique, service informatique, sans distinction de la méthode utilisée pour sa réalisation.

2.1 Saisine

Deux voies de saisines existent pour lancer le processus d'homologation d'un système d'information du MAASA.

2.1.1 Saisine par l'AQSSI

Lorsqu'un AQSSI désire mener un projet nécessitant l'homologation du système d'information de son périmètre, notamment en **préalable à toute mise en service opérationnelle d'un SI**, il saisit le Service du numérique pour initier la démarche ISP et in-fine obtenir la fiche de sécurité (annexe 4) 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.

2.1.2 Auto-saisine par le BSSI

En l'absence de saisine par l'AQSSI, le BSSI peut initier une démarche ISP visant à présenter un projet en commission d'homologation. Lorsque le système d'information a terminé le parcours de sécurité de la méthode ISP, appliquée à tous les systèmes au MAASA, le BSSI propose soumet un avis à la commission d'homologation du système d'information.

Il transmet alors à l'AQSSI ainsi qu'à l'ensemble des membres de la commission d'homologation la fiche de sécurité (annexe 4) en vue de l'homologation d'un système d'information.

2.1.3 Contenu de la « Fiche de sécurité» (cf. annexe 4)

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) Descriptif du système d'information proposé à l'homologation

Les éléments suivants doivent à minima être présents dans le dossier d'homologation :

- Objectifs fonctionnels du SI, périmètre et informations traitées, historique d'homologation(s) et catégorisation du SI (SI à enjeu au sens de la cartographie des SI à enjeu du MAASA ou non)
- Synthèse du projet (Maitrise d'ouvrage MOA, maitrise d'œuvre MOE, utilisateurs, utilisateurs droits étendus) et des travaux de sécurisation ;
- Périmètre d'homologation ;
- Date de mise en service prévisionnelle ;
- Cartographie (architecture technique, échanges de données au sein du SI, exposition du SI, modalités d'accès au SI, etc.) ;
- Sauvegardes des données ;
- Besoins de sécurité en matière de disponibilité, intégrité, confidentialité, preuve (DICP) – cf. annexe 2
- Analyse de risques de sécurité des SI ;
- Etapes ISP suivies.

2) Une fiche de synthèse de sécurité listant l'ensemble :
   - des actions de sécurité mises en œuvre ;
   - des tests de sécurité ou audits réalisés ainsi que leurs résultats communicables ;
   - des éventuelles corrections réalisées ou en cours de réalisation ;
   - des éventuels risques ou vulnérabilités résiduels.

Les mesures correctives et identifiées durant le parcours de sécurité doivent être proportionnées aux risques qu'elles sont en mesure de couvrir. A ce titre, si la mise en œuvre de la mesure coûte plus cher que le risque qu'elle couvre, il est envisageable de ne pas l'appliquer. Il en est de même si la temporalité dans laquelle s'inscrit la possibilité de mettre en œuvre la mesure dépasse le temps de vie résiduel d'une application (notamment celles en fin de vie). Ce choix est alors justifié et présenté à la commission.

Un suivi du maintien en condition de sécurité de l'ensemble des systèmes d'information du Ministère est réalisé par le SNUM, notamment sur la base des dossiers d'homologation et de l'avancement des plans d'actions qui en résultent, ainsi que de la veille effectuée sur les vulnérabilités pouvant survenir depuis la phase d'homologation.

Des engagements sont obtenus de la part des prestataires, le cas échéant, pour les SI dont la MOE est assurée par des entités externes au SNUM (prestataires, tiers, etc.).

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

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 ISP :

- 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 la fiche de sécurité (annexe 4) en vue de l'homologation d'un système d'Information, avec son avis relatif à l'homologation du système d'information.

Après validation par le chef du Service du Numérique, le BSSI transmet à l'AQSSI ainsi qu'à l'ensemble des membres de la commission d'homologation la fiche de sécurité (annexe 4) en vue de l'homologation d'un système d'information. Ce dossier complet doit être transmis à minima une semaine avant la tenue de la commission.

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.

2.2 Prononcé de l'homologation par l'AQSSI

2.2.1 Réunion de la commission d'homologation

L'AQSSI convoque les membres de la commission via le BSSI, qui assure le secrétariat.

Les débats tenus en commission d'homologation font l'objet d'un compte-rendu rédigé et diffusé par le BSSI (annexe 5).

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 en accord avec le FSSI.

Après réunion de la commission, l'AQSSI signe la décision d'homologation (annexe 6) - cf. partie dédiée.

2.2.2 Prononcé dérogatoire et exceptionnel direct de l'homologation

La réunion de la commission d'homologation est systématiquement réunie.

Par exception, si tous les membres de la Commission d'homologation font part, de manière expresse, sous la forme d'un accord sans réserve et documenté, d'une absence de commentaires, oppositions ou observations de nature à remettre en cause l'avis du BSSI, et si les enjeux de sécurité associés à l'application sont faibles, l'AQSSI peut décider de signer directement la décision d'homologation (annexe 6) transmise avec la fiche de sécurité (annexe 4). 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 3. de ce document.

2.3 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 pour une durée déterminée de 3 ans. Dans le cas où persistent de nombreux risques résiduels, cette durée peut être réduite à 6 mois ou 1 an.
- un refus d'homologation, si les résultats du dossier de sécurité font apparaître des risques résiduels jugés inacceptables.

3. Conséquences de la décision d'homologation

3.1. Mise en service

La mise en service du système intervient dès lors qu'il reçoit une décision favorable d'homologation.

Cependant, **lorsque l'urgence opérationnelle le requiert et de façon exceptionnelle**, l'AQSSI peut autoriser 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. Il convient de formaliser et transmettre les mesures de supervision spécifiques du ou des risques aux services concernés (supervision par le CSIRT Agriculture, etc.) Dans ce cas, la mise en service définitive interviendra ultérieurement, lorsque l'homologation de sécurité aura été prononcée.

3.2. Communication des décisions d'homologation

Les décisions d'homologation sont rendues accessibles au sein du MAASA par publication de la décision dans les mentions légales de l'application concernée lorsqu'il s'agit d'un service mis à disposition sur Internet (en pied de page web).

Le dossier technique est un document confidentiel qui reste en possession du BSSI, de la maitrise d'œuvre et de la maitrise d'ouvrage concernées.

Dans le cas d'un téléservice, la décision est rendue accessible aux usagers qui doivent pouvoir la consulter au sein de ce téléservice, via la mise à disposition d'une adresse de courriel permettant de contacter les équipes compétentes au sein du Ministère en charge de l'Agriculture.

3.3. Contrôle et renouvellement de l'homologation

L'autorité d'homologation (AQSSI), fixe les conditions du maintien de l'homologation de sécurité au cours du cycle de vie du système d'information. La MOA et la MOE contrôlent régulièrement que le système fonctionne effectivement selon les conditions qui ont été approuvées, en particulier après des opérations de maintien en conditions opérationnelles et de maintien en conditions de sécurité. Le maintien en conditions opérationnelles peut engendrer de nouveaux risques qu'il convient d'identifier et communiquer le cas échéant au BSSI et au CSN de l'entité. L'analyse de ou ces nouveaux risques peut entrainer la conduite d'un nouveau parcours de sécurité et donc une nouvelle homologation. Les membres de la commission d'homologation sont informés par l'AQSSI de la réalisation de ces contrôles.

L'autorité d'homologation (AQSSI) doit initier la procédure de renouvellement de l'homologation dans un délai compatible avec une ré-homologation avant le terme de la précédente (si le système d'information doit rester en production). Le BSSI assure aussi une veille et un suivi des homologations au niveau central, il alerte le cas échéant les CSN des entités un an avant l'échéance. La procédure de renouvellement est la même que celle de l'homologation initiale (cf. 2.1).

L'autorité d'homologation (AQSSI) ou le chef du Service du numérique peuvent aussi examiner 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.2.1).

La présente note garantit la sécurité et la fiabilité des systèmes d'information. Je remercie l'ensemble des services pour leur mobilisation dans la mise en œuvre de cette procédure, essentielle à la maîtrise des risques liés aux systèmes d'information.

La Secrétaire générale

ANNEXE 1 : FICHE VIERGE – PRE ETUDE DE SECURITE

MINISTÈRE
DE L'AGRICULTURE
DE L'AGRO-ALIMENTAIRE
ET DE LA SOUVERAINETÉ
ALIMENTAIRE

Liberté
Égalité
Fraternité

Secrétariat Général
Service du Numérique
Sous-direction de la Stratégie, du Pilotage et des Ressources

Pre-étude de Sécurité

Nom_Application

Ce document présente les éléments relatifs à la pré-étude de sécurité. Il est issu de la réunion du XX/XX/XXXX en présence de la MOA.

Critères DICP : **D**

Préconisations : **Préconisations**

ETAT

Etat	Acteur/Structure	Date d'état/Visa	Autres
Rédigé par	BSSI		
Relu par	AMOA		
Relu par	MOA		
Validé par			

Table des matières

1. Objectif du document

Ce document présente le résultat d'une pré-étude des besoins de sécurité du système d'information.

Ce document est issu des échanges entre le Bureau de la sécurité des systèmes d'information (BSSI) et la MOA.

Ce document devra être validé par la maîtrise d'ouvrage du système d'information qui est responsable de l'expression des besoins de sécurité du projet.

En fonction de la sensibilité des informations et des enjeux, la MOA devra prévoir de budgéter une analyse plus poussée, un plan d'action sécurité, un audit, des tests d'intrusion.

2. Organisation du projet

Les principaux acteurs du projet sont :

MOA	
AMOA	
MOE	
Prestataire	
Hébergement envisagé pour les infrastructures	

3. Rappel des objectifs et du périmètre fonctionnel

Décrire le champ d'application de l'application et ses usages

4. Planning du projet

Le tableau suivant présente les grandes phases du projet d'évolution :

Phase	Date
Spécifications Générales	
Spécifications détaillées	
Développement	
Mise en production	

5. Les utilisateurs du SI

5.1. Les populations qui vont utiliser le SI

- Lister

5.2. Les acteurs ayant des droits étendus sur le SI

Les principaux profils applicatifs prévus devant disposer de droits « fonctionnels » étendus sont :

- Administrateurs techniques :
- Hébergeurs et exploitants :

6. Les données/informations gérées par le système cible

Données Personnelles (RGPD)

- Lister

Autres données

- Lister

7. **A.P.I.**

- Cette application met-elle en œuvre des API internes (éventuellement techniques) ou externes ?

  Réponse

- Sur quel réseau ces API sont-elles exposées (RIE, Internet, etc.) ?

  Réponse

- Dans les données listées au 6, lesquelles sont exposées par les API ?

  Réponse

- Les API permettent-elles de lire, de modifier, créer ou supprimer des données ?

  Réponse

- Le destinataire des API est-il le grand public ou bien un ensemble de partenaires connus ?

  Réponse

- Les destinataires des API sont-ils authentifiés ? Si oui comment ?

  Réponse

- Des secrets, notamment d'authentification, ou bien des données confidentielles ou personnelles des usagers sont-elles véhiculées par l'API ?

  Réponse

8. Pré Analyse d'impact informatique et libertés

Les principaux points de contrôle en matière de protection des données personnelles sont :

8-1-Finalité

- Quelle est la finalité au traitement ?

  CF. Supra
- Est-elle compréhensible par tous ?

  Oui, elle est explicite

8-2-Proportionnalité

- Les données collectées sont-elles absolument nécessaires pour atteindre l'objectif fixé ?

  Oui
- Les données obligatoires et facultatives sont-elles bien distinguées ?

  Pas de données facultatives
- Des données sensibles au sens de la loi I&L et du RGPD sont-elles collectées ?

  Non
- Si oui, est-ce indispensable au regard de la finalité ?

  N/A
- Est-il possible de faire autrement ?

  N.A
- Le traitement est-il considéré comme un traitement à grande échelle ?

  Oui

8-3-Conservation

- Existe-t-il des durées de conservations ?

  Conformément à la réglementation

- Existe-t-il des règles d'archivages des données ?

  Conformément à la réglementation

- Les données sont-elles supprimées une fois qu'elles ne sont plus utiles ?

  Conformément à la réglementation

8-4-Information

- Des procédures sont-elles définies afin de faire respecter les droits des personnes fichées (information, accès, rectification, opposition et consentement exprès) ?

  Oui

- La personne exerçant son droit d'accès, de rectification ou de limitation du traitement obtient-elle satisfaction dans un délai maximum de deux mois ?

  Oui

9. Éléments d’architecture technique du projet

9.1. Référencement - Habilitation et authentification des utilisateurs :

.

9.2. Choix fondamentaux concernant l'architecture technique :

.

9.3. Application ouverte sur Internet :

.

9.4. Application ouverte sur RIE :

.

9.5. Application ouverte sur VPN ou LS :

.

10. Lien entre le système cible et d’autres SI

10.1. Échanges de données avec des SI MAASAF :

.

10.2. Échanges de données avec des SI d'autres Autorités Administratives :

.

11. Besoins de sécurité synthétiques

Recommandations

Ex : Cette application sera soumise à homologation formelle. De ce fait, et au regard des niveaux de sensibilité évoqués, le BSSI recommande la réalisation, au vu des besoins SSI :

Préconisations

Sauf avis contraire de la DPO, une analyse d'impact n'est pas nécessaire

Expression synthétique des besoins de sécurité

Critère	Niveau	Type d'impact et commentaire
Disponibilité	D	
Intégrité	I	
Confidentialité	C	
Preuve	P	

12. Pour mémoire : éléments techniques à prendre en compte

Il est essentiel de s'assurer que la solution proposée respecte les normes et politiques de sécurité en vigueur au sein du ministère. Cela implique une conformité avec les référentiels nationaux tels que le **Référentiel Général de Sécurité (RGS)**, qui établit les exigences de sécurité pour les systèmes d'information de l'administration française, ainsi que les référentiel Européen actuels et à venir.

De plus, la solution doit être conforme à la **Politique de Sécurité des Systèmes d'Information de l'Agriculture (PSSI-A)** et à la **Politique de Sécurité des Systèmes d'Information de l'Etat (PSSI-E)**, qui fournit un cadre de gouvernance pour la protection des systèmes d'information au sein du ministère.

En outre, le respect du **Règlement Général sur la Protection des Données (RGPD)** est indispensable pour garantir la protection des données personnelles traitées par la solution.

D'autres normes et bonnes pratiques, telles que celles édictées par l'**Instruction Générale Interministérielle** (**IGI) 1300** visant à empêcher la compromission d'informations dématérialisées traitées via des systèmes d'information, peuvent également être pertinentes.

Il est donc nécessaire de vérifier si la solution peut s'intégrer facilement dans notre environnement technique tout en respectant ces normes et politiques de sécurité, ou si des adaptations de notre infrastructure seront nécessaires pour sa mise en œuvre.

ANNEXE 2 : Détail des critères et niveaux d'expression des besoins de sécurité (DICP)

Le MAASA a standardisé l'expression des besoins de sécurité comme suit :

QUEL EST LE BESOIN DE DISPONIBILITE DU SYSTEME CIBLE ?

AUCUN (D0)	Ce niveau traduit un délai maximal d'interruption autorisée illimité.
FAIBLE (D1)	Ce niveau traduit un délai maximal d'interruption autorisée entre une semaine et un mois.
MOYEN (D2)	Ce niveau traduit un délai maximal d'interruption autorisée de 5 jours consécutifs ouvrés.
FORT (D3)	Ce niveau traduit un délai maximal d'interruption autorisée de 2 jours consécutifs ouvrés.
TRES FORT (D4)	Ce niveau traduit un délai maximal d'interruption autorisée de 8 heures consécutives ouvrées.
VITAL (D5)	Ce niveau traduit une tolérance inférieure à 4h.

QUEL EST LE BESOIN D'INTEGRITE DES INFORMATIONS GEREES ?

AUCUN (I0)	Ce niveau traduit qu'une perte ou modification non prévue, volontaire ou non volontaire, n'affecte en rien les activités d'un service ou d'une direction du ministère.
FAIBLE (I1)	L'exactitude des informations est avérée mais sans garantie particulière d'exhaustivité. Une sauvegarde mensuelle suffit à la récupération des données perdues. La modification illicite des informations traitées ne doit pas provoquer de gêne significative pour un service ou direction du ministère. Le contrôle visuel est suffisant pour détecter toute modification illicite.
MOYEN (I2)	L'exactitude des informations est avérée et garantie par un scellement. L'authenticité des transactions est avérée mais sans garantie particulière d'exhaustivité. Une sauvegarde hebdomadaire suffit à la récupération des données perdues. La modification illicite des informations traitées ne doit pas provoquer de gêne significative pour un service ou direction critique du ministère. Le contrôle d'intégrité est automatique et porte sur quelques éléments clés d'un traitement.
FORT (I3)	L'exactitude des informations est garantie par dispositif de scellement protégé. L'authenticité des transactions est garantie par scellement sur

	toutes les transactions. Une sauvegarde quotidienne suffit à la récupération des données perdues. La modification illicite n'est pas tolérée et doit être détectée sous 24H.
VITAL (I4)	L'exactitude des informations et l'authenticité des transactions est garantie par dispositif de scellement protégé sur l'ensemble des traitements. La modification illicite n'est pas tolérée et doit être détectée le plus rapidement possible.

QUEL EST LE BESOIN DE CONFIDENTIALITE DES INFORMATIONS GEREES ?

AUCUN (C0)	Ce niveau traduit que la diffusion d'une information dans le domaine public n'affecte en rien les activités d'un service, d'une direction du ministère ou le service public en général. Il s'agit en particulier des informations publiées sur les sites Internet institutionnels du ministère.
RESERVE INTERNE (C1)	Ce niveau traduit que la diffusion est seulement possible en interne du ministère tout service et direction confondus.
RESTREINT (C2)	Ce niveau restreint la diffusion d'information à une direction ou un service concerné ou projet transverse. Un directeur ou chef de service non concerné peut avoir accès à ce niveau de connaissance sans habilitation particulière.
CONFIDENTIEL (C3)	Ce niveau restreint la diffusion d'informations sensibles telles que des données nominatives du personnel ou d'usagers aux seuls personnels ayant le droit d'en connaître. Ces personnels doivent être listés nominativement. Un directeur ou chef de service non concerné ne peut pas avoir accès à ce niveau de connaissance sans habilitation particulière.
TRES CONFIDENTIEL (C4)	Ce niveau restreint la diffusion d'information à quelques agents pour un sujet donné. Ce niveau d'information ne devrait sortir en aucun cas du ministère.

QUEL EST LE BESOIN DE PREUVE OPPOSABLE VIA A VIS DES INFORMATIONS GEREES ?

AUCUN (P0)	Ce niveau traduit que l'absence de toute trace sur les systèmes ou applications n'affectent en rien les activités d'un service ou d'une direction du ministère. Le besoin de preuve des opérations ou des transactions effectuées sur le système est nul.

Faible (P1)	Ce niveau traduit un besoin de journalisation standard des principaux événements d'un système ou d'une application. L'élément de preuve est suffisant, il ne sera pas nécessaire de l'opposer dans le cadre d'une procédure en contentieux.
Moyen (P2)	Ce niveau traduit un besoin de journalisation systématique des accès et des entrées-sorties de données d'un système ou d'une application. L'élément de preuve est suffisant, il ne sera pas nécessaire de l'opposer dans le cadre d'une procédure en contentieux.
Important (P3)	Ce niveau traduit la nécessité une journalisation des événements systèmes ou applicatifs dont l'intégrité des journaux est garantie. L'élément de preuve doit pouvoir être produit lors d'une procédure en contentieux.
Vital (P4)	Ce niveau garantit un niveau de preuve opposable sur les événements système ou applicatifs.

ANNEXE 3 : MATRICE DE CRITICITE

Pour évaluer la criticité d'un SI, la matrice proposée par l'ANSSI dans son guide relatif à l'homologation[1] est utilisée en tant que référentiel.

L'évaluation de la criticité du SI (mineure, modérée, importante, maximale) est appréciée par le BSSI puis validée par l'AQSSI et son CSN sur la base des éléments vus durant la phase de pré-étude de sécurité (et notamment via l'évaluation des besoins de sécurité en matière de Disponibilité, Intégrité, Confidentialité, Preuve).

Sélection du niveau de la démarche d'homologation de la sécurité

	Exposition* nulle	Exposition faible	Exposition importante	Exposition totale
Criticité** maximale	Intermédiaire	Renforcé	Renforcé	Renforcé
Criticité importante	Intermédiaire	Intermédiaire	Renforcé	Renforcé
Criticité modérée	Simplifié	Simplifié	Intermédiaire	Intermédiaire
Criticité mineure	Simplifié	Simplifié	Simplifié	Intermédiaire

[1] Guide de l'homologation de sécurité des systèmes d'information publié par l'ANSSI le 1er avril 2025, page 62

ANNEXE 4 : MODELE DE DOCUMENT – Fiche de sécurité

MINISTÈRE
DE L'AGRICULTURE
DE L'AGRO-ALIMENTAIRE
ET DE LA SOUVERAINETÉ
ALIMENTAIRE

Liberté
Égalité
Fraternité

Fiche de sécurité

Application

Bureau de la sécurité des systèmes d'information

Document confidentiel - Confidentialité C3

Dossier suivi par :– BSSI*

Dossier rédigé par	BSSI	
Dossier relu par	Chef BSSI	
Dossier validé par	Sous-directeur-SPR	
Dossier validé par	Chef du Service du numérique	

TABLE DES MATIERES

PRESENTATION DU DOCUMENT

Cette fiche de sécurité analyse le besoin de sécurité du système d'information et présente la réponse apportée à ce besoin.

Des prestations de sécurité ont été jugées nécessaires par le BSSI lors de la pré-étude de sécurité et elles ont été acceptées par la maîtrise d'ouvrage. La fiche explicite la prise en compte par la Maîtrise d'Ouvrage et la Maîtrise d'œuvre des résultats de ces prestations de sécurité : les vulnérabilités détectées sont décrites et les décisions prises à leur égard sont exposées (chaque vulnérabilité est corrigée ou assumée).

La fiche contient in fine l'avis du Service du numérique concernant l'opportunité d'homologuer le système.

Pour rappel, seule la décision d'homologation de sécurité peut attester que le projet a satisfait aux exigences de sécurité et que le système d'information est apte à entrer en service avec des risques résiduels maîtrisés

OBJECTIFS FONCTIONNELS DE L'APPLICATION

[Expliciter dans cette partie à quoi sert l'application ainsi que le contexte de son utilisation (nombre structures utilisatrice, nombres services, nombres d'utilisateurs...) pour permettre d'appréhender concrètement l'utilisation de l'application]

SYNTHESE DU PROJET

- **Projet** :
- **Objectifs** :
  -
- **MOA :**
- **AMOA** :
- **MOE** :
- **Prestataire** :
- **Hébergement** :
- **Périmètre du projet :**
- **Utilisateurs :**

- **Utilisateurs ayant des droits étendus sur le SI :**

Les principaux profils applicatifs prévus devant disposer de droits « fonctionnels » étendus sont :

- **Échange de données avec d'autres autorités administratives ou des usagers :**
  -
- **Échanges de données avec des SI MAASA:**
  -
- **Données ou informations générées par le système** :
  - Autres données
    - Configurations techniques.
- **Date de mise en service** :
  - Date

ÉTAPE DE LA METHODE D'INTEGRATION DE LA SECURITE DANS LES PROJETS (ISP)

PRE ETUDE SECURITE

Date de la pré-étude :

Besoins en sécurité

Besoin	Niveau
Disponibilité	
Intégrité	
Confidentialité	
Preuve	

Mesures préconisées

Note importante : ces mesures sont imposées par la réglementation précitée.

- Réalisation d'une analyse de risque : Réalisée lors de la Pré-étude de sécurité.
- Réalisation d'un audit :
- Réalisation de tests d'intrusion :

PRESTATIONS DE SECURITE

1 / Tests d'intrusion approfondis

- **Prestataire** :
- **Objectif :.**
- **Type de tests d'intrusion réalisés :**

- **Le niveau de sécurité de l'application GRAVITEE a été évalué sur les aspects suivants** :
  - L'exposition sur Internet ;
  - La confidentialité des données ;
  - Le cloisonnement des différents profils ;
  - La robustesse des formulaires de recherche ;
  - La robustesse de l'authentification ;
  - Le filtrage des entrées ;
  - L'encodage des sorties.

- **Périmètre :**

Les tests d'intrusion ont été réalisés sur les environnements de production et de développement, depuis un accès au réseau interne du Ministère via *VPN*.

Les *URL* de l'environnement de développement qui ont été utilisées sont les suivantes :

- Adresses

Les *URL* de l'environnement de production qui ont été utilisées sont les suivantes :

- X

L'accès authentifié à l'application a aussi été évalué. Pour ce faire, les éléments suivants sont transmis par le Ministère :

Compte	Rôle

Période de tests : mois/année.

2 / Conclusions des prestations

À l'issue de l'audit, le niveau de sécurité de l'application *X* est évalué à **perfectible** compte tenu des contrôles réalisés.

En effet, durant le temps imparti à l'audit, **X vulnérabilités modérées** ont notamment été identifiées :

- X

3/ Synthèse des recommandations

A court terme :

Il est recommandé de :

- X

A moyen terme :

Il est recommandé de :

- X

A plus long terme :

Il est recommandé de :

- X

4 / Failles de sécurité mises en évidence par les prestations

ID	Titre de la vulnérabilité	Risque	Titre de la recommandation	Priorité	Complexité	Service concerné
						
						
						
						
						

	SYMBOLE	RISQUE	PRIORITE	COMPLEXITE
Légende des symboles				

5 / Proposition de plan d'actions consécutif à la prestation de sécurité

	Vulnérabilités	Service Concerné	Complément d'information du service concerné sur le traitement de la vulnérabilité	Etat

AVIS DU BSSI SUR L'HOMOLOGATION

Documents de référence

-

ANNEXE 5 : MODELE DE DOCUMENT – Relevé de décision de la commission

Relevé de décision de la Commission d'Homologation du xx/xx/xxxx

Ministère de l'agriculture, de l'Agro-Alimentaire et de la souveraineté alimentaire

Participants

La présente Commission d'Homologation s'est tenue le xx/xx/xxxx en présence de :

-
-
-

Homologations débattues lors de la commission d'homologation

Nom de l'application	Proposition de la commission	Motivation si proposition de refus d'homologation/ homologation inférieure à trois ans ou décision non conforme à l'avis BSSI

Remarques ou Observations

Signature de l'AQSSI

ANNEXE 6 : MODELE DE DOCUMENT – décision d'homologation

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

[L'AQSSI]

Objet : Décision d'homologation de l'application xxx

Vu le Décret 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,

Vu la note de service SG/SNUM/SDSPR/2023-576 du 14 septembre 2023 relative à l'homologation des Systèmes d'Information,

Vu la fiche de sécurité, établie par le Bureau de la Sécurité des Systèmes d'Information produite en vue de l'homologation de l'application « xxxx »,

Vu l'avis du Bureau de la Sécurité des Systèmes d'Information du MAASA relativement à l'homologation de l'application,

Vu l'avis de la Commission d'Homologation s'étant tenue le mercredi xx/xx/xxxx en présence de [l'AQSSI] ainsi que des personnes suivantes :

-

-

Il résulte des éléments suscités que l'application « xxx » a bien fait l'objet d'une procédure de sécurisation à l'état de l'art mise en œuvre par [l'AQSSI], procédure dont les résultats …

La Commission propose une homologation pour x ans, [éventuellement sous réserve …]

Par conséquent, l'autorité qualifiée pour la sécurité des systèmes d'information [de la structure x] décide d'homologuer l'application « xxx » pour x ans, soit jusqu'au x/xx/xxxx [sous réserve de …]

Fait à Paris, le

L'AQSSI