MINISTÈRE
DE LA JUSTICE

Liberté
Égalité
Fraternité

Guide d'homologation de la sécurité numérique des systèmes d'information

Version 2 – 2024-2025

HISTORIQUE DES VERSIONS

Version	Date	Rédacteur	Suivi des modifications
1	Mars 2024	M. HEBBAR	Harmonisation de la démarche ministérielle
2	Juin 2024	S. MICHEL	Relecture et validation

Objectif du document	Guide d'homologation de la sécurité numérique
Résumé	Ce document présente la démarche ministérielle d'homologation de sécurité numérique des services numériques au sein du ministère de la Justice en décrivant ses principes, ses étapes, ses livrables ainsi que les rôles et les responsabilités de chaque contributeur.

Table des matières

1. AVANT PROPOS

Ce guide d'homologation fait suite à la consultation des principaux acteurs de la sécurité numérique qui opèrent au sein du ministère de la Justice : FSSI, CSN et RCSSI.

Ce document a pour finalité d'accompagner chaque acteur, quel que soit le niveau et la nature de sa contribution, dans la mise en œuvre de la démarche d'homologation de sécurité numérique en application au sein du ministère.

Dans le cadre d'une démarche d'amélioration continue, ce guide évoluera et prendra en compte les retours d'expérience ainsi que tout sujet (évolution des menaces, réglementations et autres bonnes pratiques) relatif à la sécurité numérique.

1.1. OBJET DU DOCUMENT

Ce guide présente la démarche **globale** d'homologation applicable à tous les SI relevant du ministère de la Justice. Cette démarche peut être déclinée pour produire un guide spécifique à une entité ou à un environnement technique tels les SI de sûreté, industriels ou les services numériques pouvant constituer un socle (poste de travail, annuaires, sauvegardes et archivages …).
Ainsi, ce document contient et précise :

- Les principes et cas d'usage d'une homologation ;
- Le vocabulaire utilisé faisant l'objet d'un glossaire ;
- Ses étapes majeures ;
- Ses livrables ;
- Les rôles et responsabilités des principaux contributeurs (RACI).

1.2. PRINCIPES DE LA DÉMARCHE

Cette démarche d'homologation a pour objectifs majeurs de :

- **Rationaliser** et **harmoniser** une démarche à l'échelle ministérielle, commune à toutes les directions et entités relevant du ministère de la Justice ;
- **Faciliter** la déclinaison de la démarche ministérielle au regard des exigences du métier et/ou des technologies en place ;
- **S'adapter** en fonction de la criticité et des besoins de sécurité du système ;
- **Mutualiser** et **capitaliser** la production des travaux relatifs à la protection des données personnelles (dont ceux issus de l'analyse d'impact relative à la protection des données personnelles - AIPD) ;
- **Donner** la possibilité aux AQSSI, sur les conseils du CSN, de signer une décision issue d'une commission d'homologation ou en mode parapheur ;
- **Mettre en place** un dispositif global (dont organisation et outillage) permettant la mise en œuvre d'un plan d'amélioration continue de la sécurité numérique.

1.3. CAS D'USAGE

« Les infrastructures et services logiciels informatiques qui […] composent le système d'information et de communication de l'État mentionné à l'article 1er du décret du 25 octobre 2019 susvisé font l'objet de l'**homologation de sécurité** prévue à l'article 4-3 du même décret dans un délai de deux ans à compter de cette date. »[1]

En déclinaison du décret, la PMSN requiert l'homologation de tout SI dans les cas suivants :

- SI déjà en production ;
- Avant son emploi ou sa mise en production ;
- À l'expiration de son homologation en cours ;
- Avant tout mise en œuvre d'un changement majeur (technique, menace, …) affectant la sécurité numérique du SI.

Il n'est pas nécessaire de reprendre toute la démarche en cas de changement **mineur**.

Le cas échéant, seuls les **impacts du changement** dans le domaine de la sécurité seront **à actualiser** dans le dossier d'homologation.

Toute démarche d'homologation ayant démarré avant celle qui est en application pourra être **menée à son terme** dans des délais raisonnables. Il revient à l'AH ou au CSN d'évaluer l'**opportunité** de reprendre tout ou partie des éléments déjà produits.
Une mise à niveau globale sera néanmoins attendue lors de la **prochaine itération** d'homologation du SI concerné.

[1] Extrait de l'article 3 du décret 2022-513

1.4. GLOSSAIRE[2]

- **Agence Nationale Sécurité des Systèmes d'Information - ANSSI**

Autorité nationale en matière de cybersécurité. Sa mission est de comprendre, prévenir et répondre au risque cyber.

- **Analyse d'Impact relative à la Protection des Données - AIPD**

Impacts d'un traitement de données personnelles quand il est « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques[3] ».

- **Audit d'architecture**

Vérification des pratiques de sécurité relatives aux choix, positionnement et mise en œuvre des matériels et logiciels selon l'état de l'art. Ex : interconnexions.

- **Audit (ou revue) de code source**

Analyse de tout ou partie du code logiciel pour découvrir des vulnérabilités dues à des erreurs ou des mauvaises pratiques de codage. Ex : mots de passe en clair.

- **Audit de configuration**

Vérification de mise en œuvre des pratiques selon l'état de l'art en matière de configuration des dispositifs matériels et logiciels. Ex : paramétrages des serveurs.

- **Audit de sécurité physique**

Pouvant être intégrés dans les audits organisationnels, certains audits sont dédiés à l'évaluation ou la mise en conformité des emprises physiques à l'IGI 1300 et/ou des exigences applicables aux SIIV.

- **Audit organisationnel**

Évaluation du niveau de la maturité de la sécurité numérique concernant :

  - Gouvernance et organisation ;
  - Normatives, légales et réglementaires ;
  - Contractuelles vis-à-vis d'un sous-traitant ou d'un assureur.

- **Autorité d'Homologation - AH (1)**

Personne physique qui, après instruction du dossier d'homologation, prononce l'homologation du SI, c'est-à-dire, prend la décision d'accepter les risques résiduels identifiés sur le système. Elle est désignée à un niveau hiérarchique suffisant pour assumer les responsabilités qui lui incombent.

---

[2] (1) : définitions complètement ou partiellement extraites de l'IGI 1337 et/ou de l'IGI 1300

[3] Extrait de l'art. 35 du RGPD

- **Autorité Qualifiée en Sécurité des Systèmes d'Information - AQSSI (1)**

L'AQSSI est responsable de la sécurité des SI qui contribuent à l'exécution des missions dont elle a la charge. Elle ne peut déléguer cette responsabilité. À ce titre, elle est responsable, en particulier, de :

- L'élaboration et le maintien à jour d'une cartographie de ces systèmes ;
- Le maintien en condition opérationnelle et de sécurité de ces systèmes ;
- La planification des audits de sécurité de ces systèmes.

L'AQSSI alloue les ressources nécessaires pour mener à bien les projets de transformation numérique de son périmètre de responsabilité et s'assure à ce titre que les risques numériques sont gérés. Ces éléments sont tenus à la disposition du FSSI.

- **Conseiller à la Sécurité Numérique - CSN (1)**

Le CSN conseille et accompagne l'AQSSI dans l'exercice de ses responsabilités pour la gestion des risques numériques. Il peut être chargé d'accompagner les AH dans leurs démarches d'homologation. Le CSN est placé sous l'AQSSI. Sans nécessairement être un expert du domaine, il dispose d'une culture de la sécurité numérique lui permettant d'en traduire les enjeux pour le compte de son AQSSI. Le CSN s'appuie sur les compétences à disposition en matière de sécurité numérique, notamment le RSSI, le DNUM et les structures en charge du numérique. Le CSN contribue à la chaîne fonctionnelle de SSI et représente l'AQSSI dans l'instance ministérielle de pilotage de sécurité numérique.

- **Décision d'homologation (1)**

Décision prise à l'issue de la démarche d'homologation par laquelle l'AH assume les risques résiduels pesant sur le SI considéré et atteste de la capacité de ce système à traiter des informations classifiées pour un niveau de classification donné.

- **Directeur ministériel du numérique - DNUM (1)**

Définit la stratégie ministérielle du numérique dans laquelle il s'assure de la bonne prise en compte de la sécurité numérique en respectant la PMSN.

- **Expression des Besoins et Identification des Objectifs de Sécurité - EBIOS**

Méthode d'appréciation et de traitement des risques de cybersécurité conçue et publiée par l'ANSSI, en déclinaison de la norme internationale ISO 27005.

- **Fonctionnaire de sécurité des systèmes d'information - FSSI (1)**

Conseille et accompagne l'ensemble des acteurs sur les questions relatives à la sécurité numérique et pilote la mise en œuvre de la PMSN. Il contrôle l'application des exigences de sécurité numérique définies dans la PMSN, la stratégie ministérielle du numérique avec les moyens à sa disposition (par exemple les audits, les contrôles, les bilans).

Il accompagne les AQSSI dans la bonne prise en compte de la sécurité numérique sur leur périmètre de responsabilité et notamment dans l'élaboration, la mise en œuvre et la coordination des stratégies de résilience numérique, supportées par les différents plans de continuité et de reprise d'activité.

- **Loi de Programmation Militaire - LPM**

Dispositions relatives aux objectifs de la politique de défense et à la programmation financière.

- **Maitrise d'Œuvre - MOE**

Est en charge de tout ou partie de la conception, du développement, de l'exploitation ou du support d'un service numérique.

- **Maitrise d'OuvrAge - MOA**

Est en charge de faire l'interface entre le client (métier) et la MOE.

- **Maintien en condition Opérationnelle - MCO**

Le MCO vise à assurer que les actifs numériques sont disponibles et fonctionnels lorsque les usagers et opérateurs en ont besoin, évitant les arrêts non planifiés.

- **Maintien en condition de Sécurité - MCS**

Le MCS assure que le système informatique est à jour et suffisamment performant pour prévenir ou anticiper les attaques et autres actions malveillantes.

- **Politique Ministérielle de Sécurité Numérique - PMSN (1)**

Document qui définit les orientations en matière de sécurité numérique d'un ministère ou d'un établissement sous sa tutelle.

- **Prestataire qualifié pour l'audit de SSI selon le référentiel de l'ANSSI - PASSI**

Prestataire disposant de garanties concernant ses compétences et celles de son personnel, sur sa capacité organisationnelle et technique à proposer une démarche d'audit conforme aux exigences du référentiel de l'ANSSI, et sur la protection des informations sensibles dont le prestataire aura connaissance au cours de la prestation.

- **Politique de Sécurité des Systèmes d'Information – PSSI**

Politique générale ou spécifique, applicable à un organisme relevant d'un AQSSI, définissant les mesures de SSI (organisationnelles et/ou techniques) dans son ensemble.

- **RACI**[4]

Une action peut être réalisée par plusieurs acteurs mais ne peut être approuvée que par un seul. L'approbateur peut être (co-)réalisateur d'une action.

- **R - Réalisateur(s)** : personne(s) en charge de la **réalisation** d'une action ;
- **A - Approbateur** : personne **approuvant** et **garantissant** la réalisation d'une action ;
- **C - Consulté(s)** : expert(s) sollicité(s) pour avis ou compléments en retour ;
- **I - Informé(s)** : personne(s) **informées** d'une action sans attente de retour.

- **Responsable (Central) de la Sécurité des Systèmes d'Information - R(C)SSI (1)**

Le RSSI conseille et accompagne le DNUM, le CSN ou tout responsable d'une structure en charge du numérique dans la mise en œuvre opérationnelle de la sécurité numérique.
Le RSSI dispose d'une expertise technique en matière de sécurité numérique.
Le RSSI contribue à la chaîne technique et opérationnelle de la sécurité numérique.

- **Sécurité Numérique - SN (1)**

Ensemble d'activités organisationnelles, techniques ou juridiques visant à protéger et défendre les SI, ainsi que les informations qu'ils manipulent, contre d'éventuels incidents de sécurité de nature accidentelle ou intentionnelle, et à assurer la résilience numérique des entités concernées.

- **Système d'Information (et de Communication) – SI (1)**

Ensemble des infrastructures et services logiciels informatiques permettant de collecter, traiter, transmettre et stocker sous forme numérique les données qui concourent aux missions des services de l'État et des organismes placés sous sa tutelle.

- **Test d'intrusion**

Simulation en vue d'identifier les vulnérabilités pouvant être exploitées par une attaque cyber et d'en évaluer les impacts le cas échéant. Ex : utilisation d'un compte utilisateur.

[4] En Anglais : Responsible – Accountable – Consulted - Informed

2. L'HOMOLOGATION

2.1. DÉFINITION[5]

« L'homologation de sécurité est une **décision formelle** prise par l'autorité qualifiée en sécurité des systèmes d'information ou par toute personne à qui elle délègue cette fonction.
Elle atteste que les risques pesant sur la sécurité ont été identifiés et que les mesures nécessaires pour **maîtriser ces risques** sont mises en œuvre.
Elle atteste également que les éventuels **risques résiduels** ont été **identifiés** et **acceptés** par l'autorité qualifiée en sécurité des systèmes d'information. »

Le terme homologation recouvre deux notions :

- D'une part, **la démarche d'homologation** elle-même, dont l'issue est destinée à faire connaître et à faire comprendre aux autorités et aux responsables les risques liés à l'exploitation d'un système d'information ;
- D'autre part, **la décision d'homologation** par laquelle l'AH « atteste que les risques pesant sur le système d'information ont été identifiés, que les mesures nécessaires pour le protéger sont mises en œuvre et que les risques résiduels ont été identifiés et acceptés ».

L'homologation **ne protège pas** des risques numériques : elle permet aux décideurs d'en prendre conscience et de disposer d'un avis éclairé pour **décider** de leurs traitements.

C'est la démarche visant l'homologation qui permet de **maitriser** les risques.

[5] Selon le décret 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'État et de ses établissements publics

2.2. PRINCIPES CLÉS DE L'HOMOLOGATION

L'homologation d'un système d'information a pour principaux objectifs :

- Identifier et délimiter les **périmètres** (techniques et fonctionnels) du SI étudié ;
- Identifier les **acteurs** concernés, leurs rôles et responsabilités dans les phases de conception, de développement et de fonctionnement du SI, ainsi que son usage ;
- Évaluer et réduire les **écarts** de conformité qui lui sont applicables et ce, tout au long de son cycle de vie ;
- Identifier et évaluer ses **risques initiaux** et décider de leurs traitements ;
- En accepter les **risques résiduels** ;
- Définir, rationaliser, affecter et planifier les **actions** issues des différents travaux d'homologation (conformité, analyse de risques et audits) ;
- Mettre en place et **piloter** le dispositif (organisation et outils) nécessaire à la pérennisation de la **maitrise** de ces risques résiduels et de leurs évolutions potentielles.

L'**efficience** de la présente démarche d'homologation et de ses déclinaisons spécifiques est en adéquation avec le mode de développement « agile », dès lors que son dispositif (comitologie, outillage, documentation …) prévoit **systématiquement** la thématique sécurité numérique.
C'est pourquoi il est fondamental d'intégrer la sécurité des données[6] au plus tôt dans le cycle du projet, ce qui permettra d'instaurer une **confiance** au service numérique rendu et de rationaliser les **coûts** humains, financiers et techniques.

La mise en œuvre de la démarche d'homologation doit être adaptée aux enjeux de sécurité du système, notamment aux conditions générales et particulières d'usage du SI, à la nature des données manipulées et aux exigences de sécurité en termes de **disponibilité**, d'**intégrité**, de **confidentialité** et de **traçabilité**.

La présente démarche d'homologation vise à être **pragmatique** et **flexible** : la nature et la granularité des livrables seront fonction de la **criticité** du SI et de ses **exigences** de conformité et de sécurité.

[6] Dont les données à caractère personnel selon le RGPD et ses déclinaisons spécifiques

2.3. CADRE RÉGLEMENTAIRE

Conformément à la politique ministérielle de sécurité numérique du ministère de la Justice (PMSN-MJ), tout **système d'information du ministère doit être homologué**. L'homologation est obligatoire conformément aux textes en vigueur parmi lesquels :

- Le code de la défense (partie législative), notamment les articles L1332-1 à L1332-7, issus des lois de programmation militaire (**LPM**) pour les années 2015 à 2019, 2019 à 2024 (et 2024 à 2030 à venir) ;
- L'instruction générale interministérielle (IGI) n° **1300** ;
- L'instruction interministérielle (II) n° **901** ;
- La politique de sécurité des systèmes d'information de l'Etat (**PSSIE**) - circulaire n°5725/SG du 14 juillet 2014 ;
- Le règlement **910**/2014/UE sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (eIDAS) ;
- Le référentiel général de sécurité (**RGS**) - Ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

Il revient à la MOA et au CSN de la direction ou de l'entité concernée d'identifier les référentiels (textes, normes, guides ANSSI …) applicables au SI faisant l'objet de l'homologation.

La PMSN-MJ est un référentiel invariant.

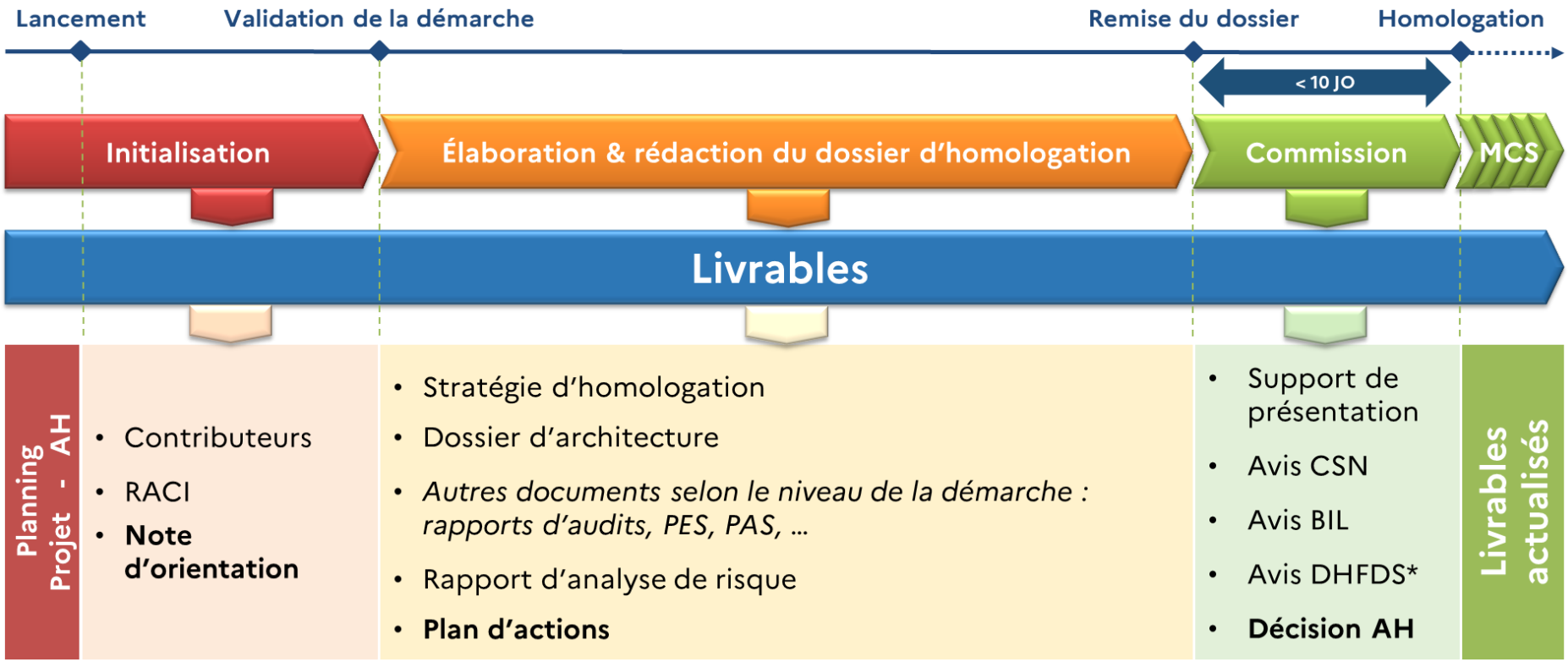
L'ensemble des **référentiels applicables** seront identifiés dans la note d'orientation et rappelés dans la stratégie d'homologation, livrables requis quel que soit le niveau de la démarche.

Toute non prise en compte d'un référentiel applicable devra faire l'objet d'une demande formelle de **dérogation** auprès du FSSI et de sa validation.

Dans le cas d'une responsabilité partagée par plusieurs AQSSI, ces dernières conviendront et désigneront une seule AH.

2.4. ÉTAPES DE LA DÉMARCHE D'HOMOLOGATION

La démarche d'homologation permet l'intégration de la sécurité numérique dès la conception et tout au long du projet.
Elle doit être considérée dès le lancement (« go ») du projet.
Les phases et étapes clés de la démarche sont schématisées par ce qui suit :



* : requis en cas de SI Essentiel ou d'Importance Vitale

3. INITIALISATION

3.1. RÉUNION DE LANCEMENT

Le chef de projet (CP) MOA s'assurera de la planification et de la préparation de la réunion de lancement de la démarche. En préparation de cette réunion, le CP MOA pré-identifiera les contributeurs (parties prenantes) du projet d'homologation.
Les objectifs majeurs de la réunion de lancement sont de :

- Présenter une synthèse des fonctionnalités globales du SI ;
- Cadrer ses périmètres (techniques et fonctionnels) ;
- Prévoir les étapes et jalons (planning prévisionnel) ;
- Confirmer les référentiels applicables ;
- Qualifier les enjeux majeurs de sécurité ;
- Identifier les contributeurs, leurs rôles et ce qui est attendu d'eux (RACI) ;
- Cadrer les prestations externes le cas échéant ;
- Rappeler la démarche d'homologation ;
- Produire le premier livrable du dossier d'homologation : la note d'orientation.

3.2. RÔLES ET RESPONSABILITÉS DES PRINCIPAUX ACTEURS

L'homologation d'un SI est l'aboutissement d'un travail collaboratif produit par un ensemble d'acteurs internes (et externes en accompagnement le cas échéant) au ministère. Au minimum, chaque projet doit avoir identifié les acteurs suivants qui seront explicitement inscrits dans la note d'orientation :

- **Chaîne décisionnelle**
  - AH : AQSSI ou personne déléguée pour décider de l'homologation du SI
- **Chaîne fonctionnelle**
  - CSN : garant des travaux d'homologation
  - CP / Rapporteur[7] homologation : CSN, CP projet (métier), CP MOA, …
- **Chaîne opérationnelle**
  - RSSI MOA ou représentant du métier
  - RSSI MOE ou représentant du fournisseur de service IT
- **Support**
  - Fonctionnaire de la Sécurité des Systèmes d'Information - FSSI
  - Déléguée Ministérielle à la Protection des Données - DMPD

[7] Le rapporteur en commission d'homologation doit être un agent du Ministère

3.3. LIVRABLE : NOTE D'ORIENTATION

La réunion de lancement doit aboutir à la production de la **note d'orientation** (également appelée note de cadrage). Actualisée jusqu'à la prochaine itération de l'homologation, elle peut constituer un chapitre dédié de la stratégie d'homologation et contiendra :

- Une description succincte du SI faisant l'objet de la démarche d'homologation ;
- Les acteurs majeurs de l'homologation : AH, CSN, CP MOA, RSSI (MOA & MOE) constituant la commission d'homologation ;
- Les référentiels applicables au SI et aux données (RGS, RGPD, directive Police-Justice, NIS 2, II 901, IGI 1300 …) ;
- Les contextes d'emploi du SI (dont exposition et interconnexions) ;
- Les exigences (dont celles relatives à la continuité d'activité) et impacts de sécurité.

La note d'orientation constituant un jalon de cadrage pour la suite de la démarche, il convient qu'elle soit transmise à toutes les parties prenantes. Il en est de même pour ses versions améliorées.

La note d'orientation est portée par le/la CSN.

En synthèse, la note d'orientation permettra d'identifier :

- Le niveau de la **démarche** d'homologation : élémentaire, standard ou renforcée ;
- Le niveau minimal **hiérarchique** de l'AH : CSN, Sous- Directeur ou DAC ;
- Les **livrables** exigibles.

3.4. NIVEAUX DE LA DÉMARCHE

La note d'orientation aura pour synthèse un tableau récapitulatif des critères de sécurité et de leurs évaluations dont la note finale déterminera le niveau de la démarche d'homologation et les livrables requis associés.
Les livrables non requis sont considérés comme optionnels par la présente démarche.
Chaque CSN peut transformer un livrable optionnel en requis.

Sauf dérogation du FSSI, un SI essentiel (**SIE**) ou d'importance vitale (**SIIV**) suivra systématiquement la démarche **renforcée**.

4. CONDUITE DE LA DÉMARCHE D'HOMOLOGATION

4.1. PRÉSENTATION DES PRINCIPAUX LIVRABLES

En plus de la note d'orientation précédemment décrite, le corpus documentaire de l'homologation d'un SI est principalement constitué des documents ci-dessous :

- **Stratégie d'homologation**

Document détaillant la démarche et ses étapes (planning prévisionnel), l'organisation, le périmètre, les acteurs et les livrables nécessaires au prononcé de l'homologation. À ce titre, l'autorité d'homologation et les membres de la commission d'homologation seront formellement désignés dans ce document.

- **Socle de conformité aux référentiels**

Souvent sous forme d'un tableau, il contient l'ensemble des mesures et exigences issues des référentiels requis et identifiés dans la note d'orientation. Ces mesures feront l'objet d'une évaluation d'application, d'une justification d'écart le cas échéant, et d'un plan de remédiation en cas d'écart non justifié.

- **Rapport d'analyse de risques**

Au cœur de l'homologation, le rapport livrera les éléments essentiels à l'identification, l'évaluation et le traitement des risques numériques permettant à l'AH d'exercer son autorité : accepter (sous condition ou pas) ou refuser les risques résiduels. Selon le SI (criticité et démarche d'homologation), le rapport intègrera tout ou partie des éléments produits par la méthode EBIOS RM[8].

- **Dossier d'architecture**

Document(s) détaillant l'architecture fonctionnelle, applicative et technique du SI cible faisant l'objet de la démarche d'homologation.

- **PSSI opérationnelle**

PSSI spécifique à un socle technique et/ou une exigence opérationnelle

- **Rapport d'AIPD**

Le cas échéant, document à produire en parallèle de l'analyse des risques en vue de rationaliser les démarches (dont l'analyse et le plan des actions de remédiation).

[8] Méthode élaborée par l'ANSSI.

- **Plan d'exploitation sécurité - PES**

Constitué des procédures d'exploitation spécifiques aux objectifs de sécurité : revue des comptes (dont comptes à privilèges), sauvegarde et restauration, arrêt et redémarrage du SI, MCO/MCS (gestion des correctifs, de la capacité, des journaux, antivirus …).

- **Rapports d'audits techniques**
  - Audit d'**architecture** : vérification des pratiques de sécurité relatives **aux choix**, positionnement et mise en œuvre des matériels et logiciels selon l'état de l'art. Ex : interconnexions de réseaux locaux ou étendus ;
  - Audit de **configuration** : vérification de mise en œuvre des pratiques selon l'état de l'art en matière de configuration des dispositifs matériels et logiciels. Ex : configuration des serveurs, systèmes ou logiciels ;
  - Audit de **code source** : analyse de tout ou partie du code logiciel pour identifier des vulnérabilités générées par des erreurs ou des mauvaises pratiques de codage. Ex : mots de passe en clair ;
  - Test d'**intrusion** : simulation en vue d'évaluer la faisabilité et les impacts d'une attaque Cyber. Ex : usurpation d'un compte utilisateur.
- **Rapport d'audit organisationnel**
  - Audit **organisationnel** : évaluation totale ou partielle des niveaux de maturité de SN concernant :
    - Gouvernance et organisation ;
    - Normes et réglementation ;
    - Contrats vis-à-vis d'un sous-traitant ou d'un assureur.
  - Sécurité **physique** : parfois intégrés dans les audits organisationnels, certains audits sont dédiés à l'évaluation des emprises physiques dans leur conformité IGI 1300.
- **Rapport d'audit de sécurité physique**

Concerne les SI de sûreté des locaux. Peut être intégré dans un audit organisationnel.

- **Procédure de gestion des incidents numériques**

Document spécifique au SI détaillant tout particulièrement les acteurs et rôles associés, en déclinaison de la PGIN ministérielle établie par le Département HFDS.

- **Plan d'assurance sécurité - PAS**

Document décrivant les engagements du prestataire dans le cas d'un recours total ou partiel de ses services. Exemples : hébergement du SI, développement, infogérance, …

- **Convention de service de supervision de sécurité**

Document précisant les modalités de la prestation de détection des incidents de sécurité réalisée par un prestataire (interne MJ ou externe) de détection d'incidents de sécurité (PDIS), qualifié par l'ANSSI selon le SI.

- **Plan d'action**

Document regroupant l'ensemble des actions issues des plans d'action (socle de sécurité, analyse de risques, audits …) à piloter pour maintenir et améliorer les objectifs et exigences de sécurité. Chaque action doit **au minimum** être définie par une **mesure**, un **porteur**, un **statut** et une **échéance** cible de réalisation.

- **Support de commission d'homologation**

Sous forme de présentation, le support sera utilisé comme fil conducteur au cours de la commission d'homologation.

- **Avis d'homologation**

Notes formalisant les positions du CSN et du FSSI concernant l'homologation d'une part, ainsi que celle de la DMPD concernant l'AIPD d'autre part. Ces notes ont pour objectif d'aider l'AH à disposer d'un avis éclairé concernant l'homologation du SI.

- **Décision d'homologation**

Note formelle de l'AH attestant de sa connaissance et de son acceptation (sous réserves le cas échéant) ou de son refus des risques résiduels du SI.

4.2. CONTRIBUTEURS

Cette matrice doit être issue de la comitologie projet et sera transcrite dans la note d'orientation.

Livrable	MOE		MOA		Support	
	CP MOE	RSSI Projet*	CP MOA	CSN	DMPD/BIL	FSSI
Note d'orientation	C	C	R	RA	I	C
Stratégie d'homologation	C	C	R	A	I	C
Socle de conformité aux référentiels	R	C	R	A	I	C
Rapport d'analyse de risques	C	C	R	A	I	C
Dossiers d'architecture (technique & fonctionnelle)	RA	R	C	C	I	I
PSSI opérationnelle	I	I	R	A	I	C
AIPD	R	C	R	C	C (BIL)	I
Plan d'Exploitation de la Sécurité - PES	C	A	I	C	I	I
Rapports d'audits techniques	R	C	C	A	I	I
Rapport d'audit organisationnel	I	I	R	A	I	C
Rapport d'audit de sécurité physique	C	C	R	A	I	C
Procédure de gestion des incidents numériques	C	C	R	A	I	C
Plan d'assurance sécurité - PAS	R	A	I	C	I	I
Convention de service de supervision de sécurité	R	C	R	A	I	I
Plan d'action	R	C	RA	C	C	C
Support de commission d'homologation	I	I	RA	C	I	C
Avis d'homologation (CSN & FSSI) et AIPD (DMPD)	I	I	C	RA	R	R
Décision d'homologation	I	I	R	RA	I	I

* RCSSI de la DNUM si pas de RSSI MOE projet nommé

4.3. SYNTHÈSE DES LIVRABLES

	Élémentaire	Standard	Renforcée
Note d'orientation	X	X	X
Stratégie d'homologation	X	X	X
Socle de conformité aux référentiels	X	X	X
Rapport d'analyse de risques	-	X (1)	X
Dossier d'architecture	X	X	X
PSSI opérationnelle	-	CSN	CSN
AIPD	BIL	BIL	BIL
Plan d'Exploitation de la Sécurité - PES	-	X	X
Rapport d'audit d'architecture	-	X	X
Rapport d'audit de configuration	-	X	X
Rapport d'audit de code (2)	-	X	X
Rapport de test d'intrusion (3)	CSN	CSN	CSN
Rapport d'audit organisationnel	-	-	XXX
Rapport d'audit de sécurité physique	-	-	XXX
Procédure de gestion des incidents numériques	-	X	X
Plan d'assurance sécurité - PAS (4)	X	X	X
Convention de service de supervision de sécurité	-	-	XXX
Plan d'action	X	X	X
Support de commission d'homologation	X	X	X
Avis d'homologation	X	X	X
Décision d'homologation	X	X	X

Légende

X : requis pour tous les SI	**- : Non requis**	**XXX : requis pour les SIIV uniquement**
CSN : à confirmer par le/la CSN		**BIL : à confirmer par le BIL**

- (1) : L'atelier 4 n'est pas requis pour la démarche standard ;
- (2) : requis si le SI est spécifiquement développé pour le Ministère (non requis dans le cas d'un progiciel) ;
- (3) : requis si le SI est exposé sur internet (un port d'écoute est actif) ;
- (4) : requis si le SI fait l'objet d'une externalisation totale ou partielle.

Dans le cas d'un SI d'importance vitale, les audits doivent être effectués par un **expert habilité au secret** (et certifié PASSI LPM).

5. HOMOLOGATION

5.1. REMISE DU DOSSIER D'HOMOLOGATION

Le CSN rédigera un avis d'homologation pour tous les SI, quel que soit le niveau de la démarche.
Pour les SI essentiels (SIE) et d'importance vitale (SIIV) uniquement, le FSSI rédigera et transmettra à l'AH un avis.
Pour cela, le dossier d'homologation complet doit avoir été chiffré (Zed !) et transmis par courriel au bureau du FSSI (cybersecurite-hfds@justice.gouv.fr) **10 jours ouvrés** avant la date prévue pour la commission d'homologation ou la pré-commission.
Les avis ont pour objectif d'aider l'AH à prendre une décision **éclairée**.

5.2. PRÉ-COMMISSION D'HOMOLOGATION

Il est recommandé de planifier une pré-commission afin de préparer la commission d'homologation si une séance de revue des livrables n'a pu se faire avec les acteurs majeurs.
Il y est présenté une synthèse des principaux livrables avant que la proposition de décision d'homologation ne soit discutée et entérinée.
L'objectif de la pré-commission est d'arbitrer tous les sujets de débat et de lever toutes les interrogations avant la tenue de la commission d'homologation formelle.
L'autorité d'homologation ne participant pas à la pré-commission, il reviendra au CSN de la présider.

5.3. COMMISSION D'HOMOLOGATION

La commission d'homologation est présidée par l'AH ou son représentant, est animée par le rapporteur (interne au ministère) et est composée de tous les contributeurs (exception faite des prestataires externes).
Sur demande expresse de l'autorité ou du CSN et par dérogation formelle du FSSI, les prestataires externes (auditeurs, consultant en accompagnement d'homologation ou d'analyse de risques …) ne pourront assister que dans la partie qui les concernent directement (ex : auditeurs).
À noter que les FSSI et DMPD (ou leurs représentants respectifs) sont membres de droit des commissions d'homologation.

La commission d'homologation **n'est pas l'instance de débats** ou de décisions techniques à prendre : le support et les échanges doivent être **axés sur le métier**.

5.4. DÉCISION D'HOMOLOGATION

Sur la base des éléments présentés au cours de la commission, l'AH pourra prononcer :

- Une homologation ferme (avec ou sans réserve, avec clause de revoyure) ;
- Une homologation provisoire (avec réserve) ;
- Un refus d'homologation.

5.4.1. Homologation ferme

La commission d'homologation présente un dossier suffisamment complet, en application de la démarche ministérielle et à celle spécifique aux contextes du SI et du métier.
L'autorité dispose de tous les éléments (socle de conformité, analyse de risques, rapports d'audits et plan d'action principalement) qui lui permettent de **connaître** et d'**accepter** les risques résiduels. Elle peut ainsi prononcer l'homologation ferme du SI pour une durée maximale de 3 ans (2 ans pour un SI classifié très secret).
La décision précisera la fréquence du comité de suivi et pilotage des risques numériques (CoSui), semestrielle au minimum pour un SI essentiel.
L'homologation ferme vaut autorisation de mise en service et autorise l'emploi du SI.

5.4.2. Homologation provisoire

La commission d'homologation a produit un dossier qui a globalement suivi la démarche d'homologation, ne permettant d'évaluer que **partiellement** les risques résiduels, faute de complétude des livrables ou d'un planning suffisamment renseigné. Toutefois, **il n'a pas été identifié de vulnérabilités critiques** pour prononcer un refus d'homologation.
La durée d'une homologation provisoire ne peut excéder 12 mois et peut exceptionnellement être renouvelée une fois pour une durée équivalente. Cette durée (2 ans au maximum) doit être mise à profit pour compléter et améliorer le dossier en vue de la prochaine commission qui devra statuer sur une homologation ferme ou un refus. La décision d'homologation provisoire devra explicitement et formellement confirmer la mise en service ou le maintien en production du système d'information, ainsi que son autorisation d'emploi.

5.4.3. Refus d'homologation

L'analyse du dossier fait ressortir que la mise en œuvre de la démarche d'homologation n'est pas suffisamment aboutie ou a révélé un risque

inacceptable compromettant significativement tout ou partie du SI du ministère.
Dans ce cas, le SI cible ne peut être mis en production (s'il est en phase projet).
Dans le cas d'un SI déjà opérationnel, il faudra prévoir :

- Un dispositif (plan d'action, usage en mode dégradé …) à effet immédiat ;
- Un décommissionnement à court terme.

> Le cas échéant, la décision de refus d'homologation confirmera **explicitement** la mise en service ou le maintien en production du système d'information, ainsi que son autorisation d'emploi.

6. POST HOMOLOGATION

6.1. SUIVI DE L'HOMOLOGATION

À l'issue de la décision d'homologation, un plan d'amélioration continue et permanente de la sécurité numérique doit être mis en œuvre et piloté via un comité (CoSui).
Présidée par le CSN, cette instance se réunira selon la fréquence validée en commission et consistera en une revue des actions figurant dans le plan. Les évolutions techniques et/ou fonctionnelles devront figurer à l'ordre du jour en vue d'évaluer les impacts dans la dimension sécurité numérique.
Les participants aux séances du comité seront fonction des points figurant à l'ordre du jour. Un compte-rendu sera rédigé à l'issu du comité, diffusé aux membres de la commission (dont l'AH, FSSI et DMPD) et pris en compte au cours du comité de gestion de risques numériques (CoGeR) tel que prévu dans la PMSN.

6.2. RENOUVELLEMENT DE L'HOMOLOGATION

Le renouvellement d'une homologation doit être initialisé lorsque :

- L'homologation en cours arrive à échéance ;
- Le système fait l'objet d'une modification majeure (périmètre, technologie, usage, etc.).

En vue d'éviter une période sans statut d'homologation, il convient de relancer la démarche au moins 6 mois avant le terme de la période en cours. Il s'agira de capitaliser l'existant et de veiller à ce que les documents soient actualisés.
Une commission d'homologation formelle devra avoir lieu.

7. ANNEXES

Annexe 1. Ateliers & étapes d'une analyse de risques EBIOS RM

Atelier	Étape	Action	Livrable
Préparation	Qualification & préparation de l'analyse de risques		Compte-rendu de lancement du projet
0.1	Qualification	Acteurs et objectifs sécurité	Note d'orientation
0.2	Planification	Planifier la réunion de lancement	Date de réunion de lancement
0.3	Lancement	Lancer le projet	Planning prévisionnel
Atelier 1	Cadrage & Socle de Sécurité		Présentation de restitution de l'Atelier 1
1.1	Cadrage	Définir le cadre de l'analyse de risques	Objectifs du projet, contributeurs, cadre temporel
1.2	Périmètres	Définir les périmètres (fonctionnel & technique)	Définition des missions, valeurs métier & biens support
1.3	Sélection	Identifier & retenir les évènements redoutés	Cartographie des évènements redoutés
1.4	Conformité	Analyser & diagnostiquer le socle de sécurité	Écarts des référentiels et mesures de remédiation
Atelier 2	Sources de Risque / Objectifs Visés (SR/OV)		Présentation de restitution de l'Atelier 2
2.1	Identification	Identifier les Sources de Risque / Objectifs Visés	Cartographie initiale des SR/OV
2.2	Cotation	Évaluer et prioriser les couples SR/OV	Cartographie intermédiaire des SR/OV
2.3	Sélection	Sélectionner les couples SR/OV	Cartographie finale des sources de risque
Atelier 3	Scénarios stratégiques		Présentation de restitution de l'Atelier 2
3.1	Identification	Identifier et évaluer les parties prenantes critiques	Cartographie de l'écosystème
3.2	Élaboration	Élaborer les scénarios stratégiques selon les ER	Cartographie des scénarios stratégiques
3.3	Remédiation	Définir les mesures de sécurité sur l'écosystème	Mesures de remédiation
Atelier 4	Scénarios opérationnels (ScOp)		Présentation de restitution de l'Atelier 4
4.1	Élaboration	Élaborer les ScOp	Cartographie initiale des ScOp
4.2	Évaluation	Évaluer la vraisemblance des ScOp	Cartographie finale des ScOp
Atelier 5	Traitement du risque		Présentation de restitution de l'Atelier 5
5.1	Synthèse	Synthétiser les scénarios de risque	Stratégie de traitement du risque
5.2	Traitement	Définir les traitements des risques	Cartographie des risques (initiaux et résiduels)
5.3	Formalisation	Évaluer et formaliser les risques résiduels	Documentation des risques résiduels
5.4	Surveillance	Mettre en place le cadre de suivi des risques	PACS
Clôture	Restitution & bilan		Recette du projet
6.1	Restitution	Rédiger le rapport final	Rapport final de l'analyse des risques

Annexe 2. Détails des rôles et responsabilités des acteurs

Au ministère de la Justice, l'AQSSI[9] peut être :

- La secrétaire générale du ministère ;
- Les directeurs d'administration centrale ;
- L'inspecteur général, chef de l'inspection générale de justice ;
- Le directeur ministériel du numérique ;
- Le secrétaire général du Conseil d'État ;
- Le directeur ou chef de service d'un service à compétence nationale rattaché directement au ministre ou à caractère interministériel ;
- Les personnes exerçant des fonctions de direction générale des établissements publics sous-tutelle ;
- Les personnes exerçant des fonctions de direction générale des autorités administratives indépendantes et des autorités publiques indépendantes.

L'**AQSSI** est responsable de la sécurité des systèmes d'information au sein de sa direction, du service, de l'établissement ou de l'autorité. **Sa responsabilité ne peut être déléguée**.
Elle s'assure, à ce titre, de l'application des instructions ministérielles données en cette matière, sous l'autorité du haut fonctionnaire de défense et de sécurité (HFDS).
Dans ce cadre, en liaison avec le HFDS et le FSSI qui lui est rattaché, l'autorité qualifiée doit :

- Disposer d'une analyse, régulièrement mise à jour, des risques encourus par les SI de sa structure ;
- S'assurer que des contrôles internes de sécurité sont régulièrement effectués ;
- Organiser la sensibilisation et la formation du personnel aux questions de sécurité, en particulier en matière de systèmes d'information ;
- Désigner les autorités d'homologation des systèmes et des services numériques relevant de sa responsabilité.

Lorsque l'AQSSI ne désigne pas d'AH, elle assure elle-même ce rôle.

L'AQSSI assurera elle-même l'autorité d'homologation d'un SIIV.

L'**AH** est représentée par des fonctions différentes selon le SI. Elle a pour mission de :

- Présider la commission d'homologation ;

[9] Arrêté du 17 février 2020 - portant désignation des AQSSI.

- Contrôler la prise en compte de la bonne intégration de la sécurité dans toutes les phases du cycle de vie du projet ;
- Prendre la décision d'accepter les risques résiduels qui pèsent sur le système ;
- Prononcer la décision d'homologation.

Qui peut être autorité d'homologation ?

- L'AQSSI pour tous les SI et **uniquement** l'AQSSI pour les **SIIV** (dont la démarche renforcée est requise) ;
- Un chef de service (sous-directeur ou équivalent) pour les SI concernés par une démarche élémentaire, standard ou renforcée (SI essentiel uniquement) ;
- Le CSN pour les SI éligibles à une démarche d'homologation élémentaire.

Le **CSN** conseille et accompagne l'AQSSI dans l'exercice de ses responsabilités en matière de procédures d'homologation.

- En charge de la sécurité du système cible d'un point de vue stratégique, il représente la MOA de la sécurité du projet. Il a pour mission de s'assurer de l'intégration de la sécurité numérique dans les projets, de conseiller l'AQSSI concernant l'homologation d'un système et de piloter les plans d'actions décidés en commission d'homologation.
- Lorsque l'AQSSI désigne une AH, le CSN exerce sa mission de conseil et d'accompagnement au profit de cette AH.

Le **RSSI MOA** ou **RCSSI** s'assure de la mise en œuvre opérationnelle des moyens et des procédures techniques permettant de répondre au besoin de sécurité du système cible, notamment de l'intégration effective des éléments techniques permettant de répondre au besoin de sécurité. Concernant les éléments techniques, il assure l'interface entre la MOA et la MOE, le CP MOA et le CSN ne disposant pas forcément d'un niveau suffisant de connaissances techniques.

Le **RSSI MOE** pilote la maitrise d'œuvre du projet et l'exploitation sécurisée du SI sur le plan technique. En général, ce rôle est assumé par un représentant de la DNUM.

Cas particulier
Le responsable du BSSI au sein de la DNUM a deux rôles distincts :

- CSN de la DNUM si cette fonction n'est pas assurée par une autre personne et lorsque le SI à homologuer relève de la DNUM, ie lorsque l'AQSSI est le DNUM ;
- RCSSI MOE concernant les SI ne relevant pas de la DNUM.