

GUIDE D'HOMOLOGATION DE SECURITE

Guide d'intégration de la sécurité dans les projets

RÉF : – 3

Destinataires

Equipe sécurité
Directeur /Chef de projet MOE /MOA
AQSSI
RSSI MOA/MOE

| <i>Version - Date</i> | <i>Emetteur</i> | <i>Statut/Suivi des modifications</i> |
|-------------------------------|-----------------|--|
| V.0.8 - projet Mai 2019 | HFDS/FSSI | Formalisation du guide |
| V.0.9 – projet Juin 2013 | HFDS/FSSI | Intégration des remarques DPJJ/DSJ/SSIC |
| V 1.0 Juillet/octobre 2019 | HFDS/FSSI | Intégration des commentaires complémentaires |

Objectif du document

Guide d'homologation en vigueur au ministère de la justice.

Mots clefs

Homologation des systèmes d'information (SI)

Résumé

Ce document présente la procédure d'homologation des SI au sein du ministère de la justice, ses grandes étapes, les rôles et les responsabilités de chacun.

Sommaire

| | | |
|----------|---|-----------|
| 1 | OBJECTIFS | 3 |
| 2 | DELIMITER LE PERIMETRE DE L'HOMOLOGATION | 5 |
| 3 | IDENTIFIER LES ACTEURS DE LA SECURITE | 6 |
| 4 | DETERMINER LE NIVEAU DE SENSIBILITE DU SYSTEME..... | 8 |
| 5 | CONSTITUER LE DOSSIER D'HOMOLOGATION | 9 |
| 6 | PREPARER ET TENIR UNE COMMISSION D'HOMOLOGATION | 12 |
| 7 | ANNEXES..... | 14 |
| | Annexe 1 : fiche d'évaluation à la sécurité d'un projet..... | 1 |
| | Annexe 2 : stratégie d'homologation type..... | 10 |
| | Annexe 3 : procédure de gestion des risques..... | 21 |
| | Annexe 4 : procédure d'exploitation de sécurité type | 42 |
| | Annexe 5 : décision d'homologation type | 51 |

1. OBJECTIFS

Ce guide a vocation à présenter la démarche d'homologation d'un système d'information. Celui-ci permet de garantir un niveau de sécurité acceptable du système considéré :

- en trouvant un équilibre entre les risques acceptables et les coûts nécessaires au renforcement de la sécurité ;
- en s'assurant que les risques pesant sur le SI, dans son contexte d'utilisation, sont connus et maîtrisés.

La mise en œuvre de la démarche d'homologation permet au ministère de la justice de se mettre en conformité avec les textes en vigueur en matière de cybersécurité et en particulier :

- **le règlement général sur la protection des données (RGPD n° 2016/679)** ;
- **le référentiel général de sécurité (RGS)**, arrêté (NOR: PRMD1413745A) du 13 juin 2014, pour les systèmes permettant des échanges entre une autorité administrative et les usagers ou entre autorités administratives ;
- **l'instruction générale interministérielle n° 1300** (IGI-1300), arrêté du 30 Novembre 2011, pour les systèmes traitant d'informations classifiées de défense ;
- **la politique ministérielle de défense et de sécurité (PMDS V9)**, arrêté ministériel du 18/08/2016 ;
- **la politique de sécurité des systèmes d'information de l'Etat (PSSIE)**, circulaire du Premier ministre n° 5725/SG (NOR : PRMX1420095C) du 17 juillet 2014, pour les systèmes des administrations de l'État.

Ces textes qui s'appliquent au périmètre du ministère de la justice, imposent qu'une décision d'homologation soit prononcée par l'autorité d'homologation avant la mise en service de chaque système d'information.

La décision d'homologation est l'engagement par lequel l'autorité d'homologation (constituée au sein de l'autorité administrative) atteste 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, et que le système d'information est donc apte à entrer en service.

Le terme homologation recouvre deux donc notions :

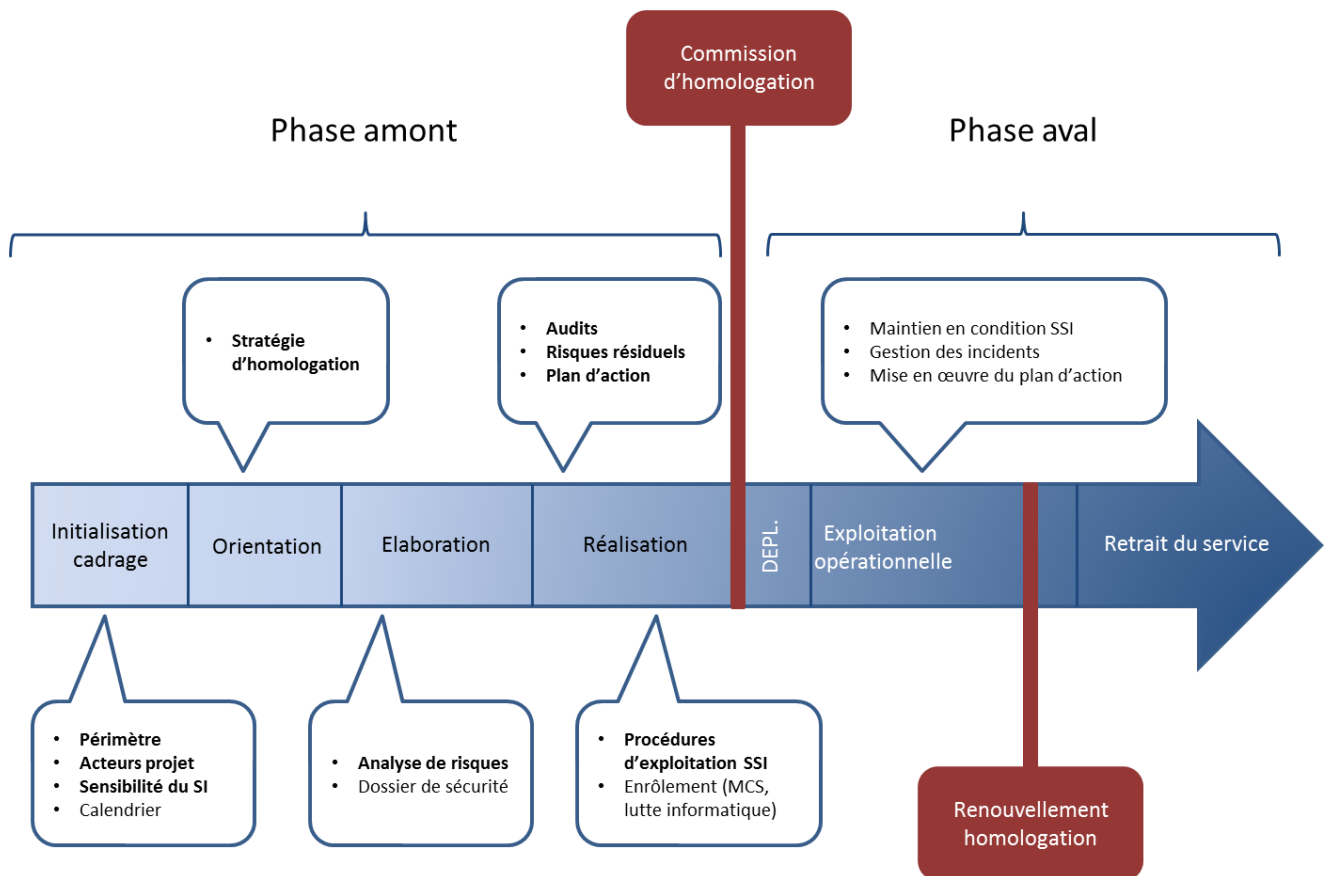
- la démarche d'homologation, destinée à faire connaître et faire comprendre aux responsables les risques liés à l'exploitation d'un système d'information ;
- la décision d'homologation soutenue par la constitution d'un dossier de sécurité et qui conclut la démarche.

L'homologation doit être adaptée aux enjeux de sécurité du système, notamment au contexte d'emploi, à la nature des données contenues, ainsi qu'aux besoins des utilisateurs :

- dans les cas de systèmes complexes ou à fort enjeu de sécurité, il est souhaitable que le responsable s'entoure d'experts techniques et fonctionnels (la commission d'homologation). Il peut déléguer la prise de décision à l'un de ses représentants qui présidera ce comité d'experts ;
- dans le cas de systèmes simples, le responsable peut mettre en place des procédures simplifiées associant un nombre plus limité d'acteurs (Cf. Annexe 2 : Stratégie d'homologation type).

S'agissant plus spécifiquement de la conformité à la réglementation sur la protection des données personnelles du système d'information, elle peut avoir un impact sur la conception même de l'outil. Il est donc indispensable d'associer à tout projet, en amont, le bureau informatiques et libertés (SG/SEM/SDAJGCSE/BIL) et le délégué à la protection des données (dpd@justice.gouv.fr).

La **démarche d'homologation** participe à l'intégration de la sécurité tout au long du projet. Pour cela, elle **doit être lancée en amont puis être totalement intégrée au projet dès les phases d'orientation et d'élaboration du SI.**



• Figure 1 : phases d'intégration de la sécurité dans le projet

2. DELIMITER LE PERIMETRE DE L'HOMOLOGATION

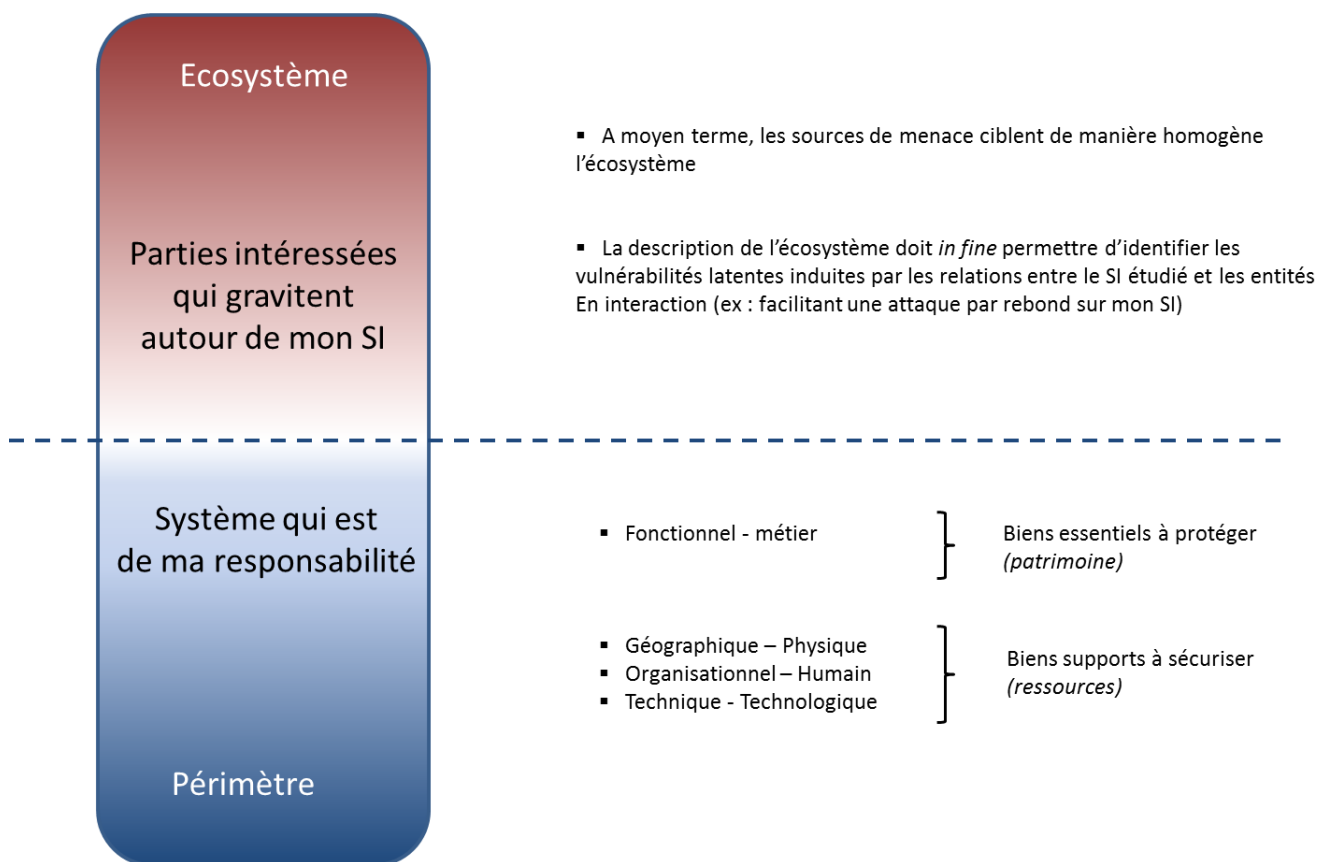
Le périmètre du système d'information à homologuer doit comporter tous les éléments indispensables au fonctionnement du système. La délimitation du périmètre ne doit comporter aucune ambiguïté, car elle permet de déterminer et de caractériser précisément le ou les systèmes qui seront homologués.

La description de ce périmètre **comprend** :

- des **éléments fonctionnels et d'organisation** : fonctionnalités du système, type d'utilisateurs, contexte et règles d'emploi, procédures formalisées, conditions d'emploi des produits de sécurité, gestion des droits, dispositifs de détection et de gestion des incidents ;
- des **éléments techniques** : architecture du système (en précisant notamment les interconnexions avec d'autres systèmes), possibilité d'utilisation de supports amovibles, d'accès à distance ou de cloisonnement, mécanismes de maintenance, d'exploitation ou de télégestion du système, notamment lorsque ces opérations sont effectuées par des prestataires externes ;
- le **périmètre géographique et physique** : localisations géographiques et caractéristiques des locaux.

Le périmètre peut évoluer au cours de la démarche d'homologation, mais il est recommandé d'aboutir rapidement à une **délimitation stable** de celui-ci.

L'ampleur de la démarche à engager sera graduée en deux niveaux (homologation simple ou homologation avancée) selon la sensibilité du système considérée.



• Figure 2 : délimitation du périmètre

3. IDENTIFIER LES ACTEURS DE LA SECURITE

Le directeur ou le chef de projet (DPOCP) : le DPOCP de la maîtrise d'ouvrage (MOA) a en charge le pilotage des travaux relatifs à l'homologation du système que ce soit en phase projet ou lorsque celui-ci est en production.

L'autorité qualifiée pour la sécurité des systèmes d'information (AQSSI) : l'AQSSI est la personne responsable, pour sa structure, de la sécurité des systèmes d'information. Elle est chargée entre autres, avec le fonctionnaire de sécurité des systèmes d'information (FSSI):

- de disposer d'une analyse des risques encourus par le SI de sa structure, et de la mettre régulièrement à jour,
- de décliner la politique ministérielle de sécurité des SI adaptée aux spécificités de sa structure et d'en fixer les objectifs,
- de s'assurer que les dispositions réglementaires et contractuelles sur la sécurité des SI sont appliquées.

Au ministère de la justice, le secrétaire général, le secrétaire général du conseil d'état, les directeurs d'administration centrale ayant autorité sur un opérateur d'importance vitale, les directeurs généraux des établissements publics sous tutelle sont les autorités qualifiées responsables de la conduite opérationnelle des politiques de sécurité des systèmes d'information.

L'autorité d'homologation : l'autorité d'homologation est une personne physique qui, après instruction du dossier d'homologation, prononce l'homologation du système c'est-à-dire qu'elle prend la décision d'accepter les risques résiduels qui pèsent sur le système. Son rôle est de :

- mettre en place et présider la commission d'homologation ;
- contrôler la prise en compte de la bonne intégration de la sécurité dans toutes les phases du cycle de vie du projet.

L'AQSSI doit désigner les autorités d'homologation responsables des systèmes d'information. L'autorité d'homologation doit être à un niveau hiérarchique suffisant pour assumer toute les responsabilités (chef de service, sous-directeur ou directeur projet/programme). Cette autorité mettra en place et présidera la commission d'homologation.

Si aucune autorité d'homologation n'a été officiellement désignée, l'AQSSI endosse par défaut cette responsabilité. Elle assumera ainsi de manière exceptionnelle les deux fonctions.

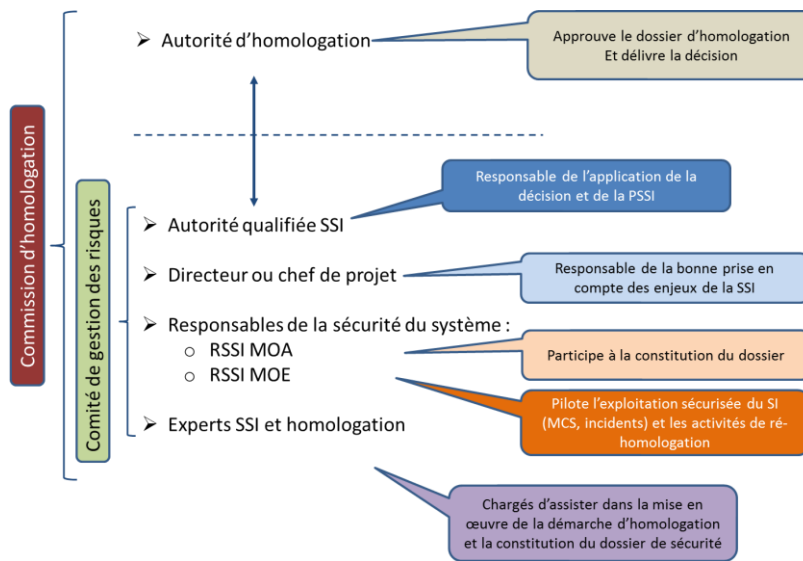
La commission d'homologation : composée des membres du comité de gestion des risques et présidée par l'autorité d'homologation, la commission est chargée de préparer la décision d'homologation.

Le comité de gestion des risques : ce comité réunit les représentants de la MOA et des équipes SSI fonctionnelles et opérationnelles, dont la responsabilité est d'accepter les niveaux de risques résiduels, les solutions de traitement proposées pour réduire les risques majeurs, arbitrer lorsqu'elle est complexe la solution de traitement des risques majeurs. Son objectif est également de départager et d'appuyer la solution retenue pour « débloquer » un risque dont le traitement est « bloqué ». Pour cela, la présence de l'AQSSI permettra d'arbitrer la solution à retenir.

Le comité de gestion des risques est composé des membres suivant :

- le **directeur ou le chef de projet** de la maîtrise d'ouvrage ;
- l'**AQSSI** (en tant que de besoin) ;
- le **RSSI de la maîtrise d'ouvrage (MOA)** ;
- Le responsable d'exploitation du système ;
- Le **RSSI de la maîtrise d'œuvre (MOE)** ;
- Les partenaires et les prestataires.

Les processus attribués au comité de gestion des risques sont définis dans le document [Procédure de gestion des risques].



• Figure 3 : Gouvernance de la sécurité dans le projet

4. DETERMINER LE NIVEAU DE SENSIBILITE DU SYSTEME

Un outil de diagnostic proposé en annexe 1 permet au DPOCP de la MOA d'évaluer le niveau de sensibilité du système en estimant :

- le dimensionnement du projet ;
- les besoins de sécurité du métier ;
- la portée du projet en termes d'objectifs métiers et d'utilisation des ressources ;
- le nombre d'utilisateurs ;
- les technologies utilisées.

Trois niveaux de sensibilité peuvent être atteints :

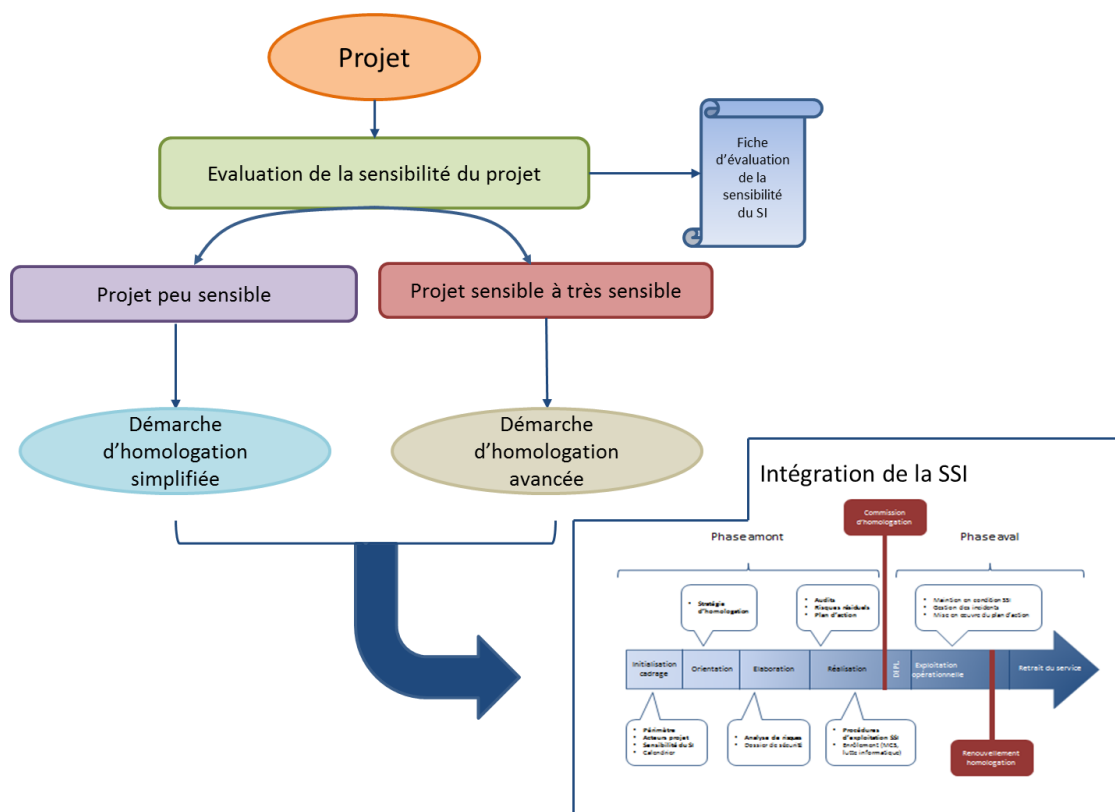
- niveau 1 : très sensible ;
- niveau 2 : sensible ;
- niveau 3 : peu sensible.

Cet outil offre la possibilité de contrôler la cohérence du projet entre les ressources disponibles (en termes de budget et de temps) et son niveau de sensibilité.

Un projet se trouvant en état de non cohérence mettra en danger les ressources du ministère, car les risques pesant sur les actifs ne pourront être réduits. Il conviendra donc de réévaluer les ressources jusqu'à l'obtention d'un état de cohérence approprié.

L'outil est utilisé par le chef ou le directeur de projet en lien avec les acteurs concernés. Les résultats sont présentés au comité de gestion des risques qui prendra la décision d'opter pour une démarche d'homologation simplifiée ou avancée.

Le niveau de sensibilité du projet déterminé conditionnera la démarche d'homologation à suivre (homologation simple ou homologation avancée).



• Figure 4 : mesure du niveau de sensibilité du SI

5. CONSTITUER LE DOSSIER D'HOMOLOGATION

Le contenu du dossier variera selon le niveau de sensibilité du système. Le tableau ci-dessous synthétise les éléments constitutifs du dossier d'homologation :

| | Homologation simple | Homologation avancée | Sensibilité |
|---|---------------------|----------------------|--|
| Stratégie d'homologation | Indispensable | | Diffusion restreinte |
| Référentiel réglementaire applicable | Indispensable | | Non protégé |
| Analyse de risques formalisée | Recommandée | Indispensable | Diffusion restreinte Ou Confidentiel défense |
| Objectifs de sécurité | Indispensable | | Non protégé ou Diffusion restreinte - |
| Politique de sécurité des SI | Recommandée | Indispensable | Non protégé ou Diffusion restreinte |
| Procédures d'exploitation sécurisée | Indispensable | | Non protégé ou Diffusion restreinte |
| Dossier d'architecture technique | Indispensable | | Diffusion restreinte |
| Résultats d'audits | Indispensable | | Diffusion restreinte |
| Plan d'action | Indispensable | | Diffusion restreinte |
| Liste des risques résiduels | Indispensable | | Diffusion restreinte |
| La proposition de décision d'homologation du SI | Indispensable | | Non protégé |
| Décisions d'homologation des systèmes interconnectés au SI | Recommandée | Indispensable | Non protégé |
| Journal de bord de l'homologation | Recommandée | Indispensable | Non protégé |
| Compléments pour les Systèmes existants | | | |
| Tableau de bord des incidents et de leur résolution | Recommandé | Fortement recommandé | Non protégé |
| Journal des évolutions du système | Recommandé | | Non protégé |

La stratégie d'homologation, pouvant être constituée à un stade liminaire en phase d'initialisation du projet, doit permettre à l'autorité d'homologation et aux acteurs participants à l'intégration de la sécurité dans le projet d'identifier sans ambiguïté :

- le cadre réglementaire applicable ;
- le périmètre d'homologation ;
- les besoins de sécurité des fonctions et services du SI et des données traitées ;
- la démarche d'identification des risques et d'homologation (méthodologie, articulation, phase) ;
- les différents acteurs impliqués, leur responsabilité et la composition de la commission d'homologation ;
- le contenu du dossier d'homologation ;
- le calendrier du plan de remédiation.

La stratégie d'homologation est rédigée par le chef ou le directeur de projet de la MOA en lien avec les RSSI MOA et MOE. La stratégie d'homologation sera soumise à la validation de la commission d'homologation et à l'approbation de l'autorité d'homologation.

Une stratégie d'homologation type est proposée en annexe 2.

Les principaux **textes réglementaires applicables** sont :

- **le règlement général sur la protection des données (RGPD n° 2016/679)** ;
- **le référentiel général de sécurité (RGS)**, arrêté (NOR: PRMD1413745A) du 13 juin 2014, pour les systèmes permettant des échanges entre une autorité administrative et les usagers ou entre autorités administratives ;
- **l'instruction générale interministérielle n° 1300** (IGI-1300), arrêté du 30 Novembre 2011, pour les systèmes traitant d'informations classifiées de défense ;
- **la politique ministérielle de défense et de sécurité (PMDS V9)**, arrêté ministériel du 18/08/2016 ;
- **la politique de sécurité des systèmes d'information de l'Etat (PSSIE)**, circulaire du Premier ministre n° 5725/SG (NOR : PRMX1420095C) du 17 juillet 2014, pour les systèmes des administrations de l'État.

Il sera nécessaire, si besoin, de compléter cette liste par les textes réglementaires spécifiques au « métier ».

L'**analyse de risque** formalisée doit se baser sur la méthode EBIOS (2010 ou « Risk Manager »).

Une procédure de gestion des risques adaptée à l'environnement du ministère de la justice est proposée en annexe 3.

La **politique de sécurité du système d'information** (PSSI) précise les exigences techniques et organisationnelles de sécurité du système d'information. Il s'agit du document de référence applicable à l'organisme, à la direction, voire dédié à un système. La PSSI présente :

- les éléments stratégiques ;
- le périmètre du SI, les enjeux liés, les orientations stratégiques ;
- les mesures de sécurités par domaine (organisationnel, technique).

La PSSI est rédigée conjointement par le RSSI MOA et le RSSI MOE. La PSSI est validée par l'AH. Cette politique est complétée par des procédures d'exploitation de la sécurité.

Les **procédures d'exploitation de la sécurité** (PES) traduisent de manière opérationnelle en mesures les objectifs de sécurité. Ces procédures doivent être détaillées et directement applicables. Ces procédures sont établies par les équipes d'exploitation et validées par le RSSI MOE.

Le document traite entre autres du maintien en condition de sécurité et lutte informatique défensive sur tout le cycle de vie du SI. Afin de respecter le besoin d'en connaître, le document doit idéalement être scindé en deux parties : l'une dédiée aux utilisateurs, l'autre aux administrateurs.

Il est recommandé que l'autorité d'homologation s'assure, au travers d'un dossier de recette, que ces procédures ont été testées avec succès avant de prononcer l'homologation. Une trame de PES figure en annexe 4.

Le **dossier d'architecture** technique (DAT) décrit l'architecture détaillée mise en œuvre dans le SI, pour répondre aux objectifs de sécurité. Il présente les composants d'infrastructure (matériels, logiciels, réseau) nécessaire à la construction du SI et précise la manière avec laquelle ils sont mis en œuvre pour ce système. Le document peut aussi bien traiter de la partie utilisateur de celle administrateur. Le dossier d'architecture est constitué par les architectes techniques du projet puis validé par le RSSI MOE.

Les **résultats d'audits** : les audits techniques et organisationnels doivent porter sur les mesures de sécurité liées à l'exploitation du système et les comparer à l'état de l'art. La réalisation d'audits, permet de mesurer les écarts entre les risques hypothétiques issus de l'analyse de risques et la réalité du terrain. L'audit mène à l'établissement d'une liste de vulnérabilité et **un plan d'action associé**. Les audits peuvent être réalisés par des équipes internes ou externes au ministère de la justice, sous pilotage du RSSI MOE. Dans tous les cas, ils ne doivent pas dépendre de la structure projet.

Les différents types d'audits pouvant être réalisés sont, par ordre de priorité décroissante :

- audit d'architecture ;
- audit de configuration ;

- audit de code ;
- tests de pénétration.

La **liste des risques résiduels** : ce document établit la synthèse des risques résiduels identifiés pour le système. Cette liste est établie par le directeur ou le chef de projet en lien avec les RSSI. En fonction du stade d'avancement de la démarche d'homologation, ce document contient le bilan des risques résiduels issus :

- des travaux amont de l'analyse de risques, d'architectures et d'infrastructures (risques résiduels par conception) ;
- des travaux de conformité à la réglementation (écarts à la réglementation identifiés) ;
- des audits et contrôles SSI (vulnérabilités et risques résiduels mesurés).

L'homologation est principalement prononcée sur la base de l'acceptation de ces risques par l'autorité d'homologation.

Les **décisions d'homologation des systèmes interconnectés** : dans l'hypothèse où les systèmes interconnectés au SI considéré ont fait l'objet d'une homologation, les décisions afférentes peuvent ou doivent être intégrées au dossier d'homologation. Ces décisions sont prises par les autorités d'homologation des maitrises d'ouvrage concernées.

La **proposition de décision d'homologation** est constituée par la commission d'homologation sur la base des travaux réalisés par le comité de gestion des risques. Cette proposition est présentée en commission d'homologation à l'autorité d'homologation pour approbation.

La proposition d'homologation présente :

- le périmètre de l'homologation ;
- la durée d'homologation ;
- les conditions éventuelles accompagnant l'homologation (l'homologation est permise sous réserve de la mise en œuvre d'un plan d'action dont les échéances et les responsables sont identifiés).

Modèle de RACI pour le ministère de la justice

| | ExP | BAPT | RSSI MOA | RSSI MOE | CPODP MOA | AH | AQSSI | BIL |
|--|-----|------|-------------|-------------|--------------|----|-------|-----|
| Stratégie d'homologation | I | I | C | C | R | A | I/C | C |
| Référentiel réglementaire applicable | I | I | C | C | R | A | I/C | C |
| Analyse de risques formalisée | I | I | R | C | C | A | I/C | C |
| Objectifs de sécurité | I | I | R | C | C | A | I/C | C |
| Politique de sécurité des SI | I | C | R | R | I | A | I/C | I |
| Procédures d'exploitation sécurisée | R | I | C | A | I | I | I | I |
| Dossier d'architecture technique | I | R | C | A | I | I | I | I |
| Résultats d'audits | I | I | I | R | A | I | I | I |
| Plan d'action | C | C | C/R | C/R | A | I | I | I |
| Liste des risques résiduels | I | I | C | C | R | A | I/C | C |
| La proposition de décision d'homologation du SI | I | I | C | C | R | A | I | C |
| Décisions d'homologation des systèmes interconnectés au SI | I | I | C | C | R | A | I | I |
| Journal de bord de l'homologation | I | I | A | I | R | I | I | I |
| Tableau de bord des incidents et de leur résolution | C/I | C/I | A | R | C | I | I | I |
| Journal des évolutions du système | C/I | C/I | C | C | R | A | I | I |

A : approuve, R : réalise, C : consulté, I : informé

6. TENIR UNE COMMISSION D'HOMOLOGATION

La commission d'homologation assiste l'autorité d'homologation pour l'instruction de l'homologation et est chargée de préparer la décision d'homologation. A cette fin, elle élaborera un support de présentation reprenant l'ordre du jour décrit ci-après. Sa composition est décrite en annexe 2 « stratégie d'homologation type » au point 3.3 page 15.

Pour cela, elle constitue un dossier de sécurité complet visé et validé par le comité de gestion des risques qu'elle fournira et présentera à l'autorité d'homologation. Le dossier pourra être transmis aux participants quinze jours avant la tenue de la commission. La tenue de la commission d'homologation est à l'initiative du DPOCP. Elle est présidée par l'autorité d'homologation.

Lors d'une commission les éléments suivants sont présentés :

Description du contexte

- Présentation du système : historique, missions, concept d'emploi, schéma technico-opérationnel, écosystème, sites de déploiement et zones d'implantation ;
- Composition de la commission d'homologation (rôles et responsabilité des acteurs) ;
- Démarche d'homologation et corpus documentaire du dossier de sécurité.

Revue des risques résiduels

- Analyse de risques : besoins de sécurité, scénarios de risques les plus significatifs ;
- Synthèse des résultats d'audits et mises en exergue des vulnérabilités critiques identifiées ;
- Revue formelle des risques résiduels décrits dans document idoine.

Plan d'action

- Description du plan d'action en identifiant les délais courts/moyens/longs terme et les responsables.

Gouvernance de la gestion de risque

- Organisation de la gestion des risques ;
- Indicateurs de pilotage (Si existants).

Proposition de la décision d'homologation

- Un exemple de proposition d'homologation figure en annexe 5.

Sur la base de ces éléments, l'autorité d'homologation pourra prononcer :

- une homologation pour une durée déterminée (de 1 à 5 ans) ;
- une homologation provisoire (de 6 mois à 1 an), ou autorisation provisoire d'emploi, assortie de réserves et d'un délai de mise en conformité des défauts de sécurité rencontrés ;
- un refus d'homologation, si les risques résiduels sont jugés inacceptables.

Dans le cas d'une homologation provisoire ou d'un refus d'homologation, l'autorité précisera les conditions (niveau de sécurité à atteindre, délai, responsable), assorties d'un plan d'action, pour lesquelles le système devra se conformer avant d'entrer en production.

Après la tenue de la commission d'homologation, le DPOCP rédigera le compte-rendu et la proposition d'avis de commission d'homologation (cf. annexe 5 : décision d'homologation type) qu'il soumettra à la signature de l'autorité d'homologation.

Un exemple d'organisation d'une homologation est présenté en annexe 2 [Stratégie d'homologation type] du présent document.

Glossaire

AH : autorité d'homologation

ANSSI : agence nationale de sécurité des systèmes d'information

APE : autorisation provisoire d'emploi

AQSSI : autorité qualifiée pour la sécurité des systèmes d'information

BAPT : bureau des architectures et des projets transverses du ministère de la justice

BIL : bureau informatique et liberté

CERT-FR : centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques

CPODP : Chef de projet ou directeur de projet

DAT : dossier d'architecture technique

DdA : la déclaration d'applicabilité

DSI : direction des systèmes d'information

DPOCP : directeur ou chef de projet

EBIOS : expression des besoins et identification des objectifs de sécurité

ExP : département exploitation et production du ministère de la justice

FISEC : fiches d'incidents de sécurité

FSSI : fonctionnaire de la sécurité des systèmes d'information

IGI 1300 : instruction générale interministérielle n°1300

ITSEC : Information Technology Security Evaluation Criteria

MOA : maîtrise d'ouvrage

MOE : maîtrise d'œuvre

PES : procédure d'exploitation de la sécurité

PMDS : politique ministérielle de défense et de sécurité

PSSIE : politique de sécurité des systèmes d'information de l'Etat

RGPD : règlement général sur la protection des données

RGS : référentiel général de sécurité

RSSI : responsable de la sécurité des systèmes d'information

SSIC : service des systèmes d'information et de communication

6. ANNEXES

- **Annexe 1 : Fiche d'évaluation de la démarche d'homologation d'un projet**
- **Annexe 2 : stratégie d'homologation type**
- **Annexe 3 : procédure de gestion des risques**
- **Annexe 4 : procédure d'exploitation de sécurité type**
- **Annexe 5 : décision d'homologation type**

Annexe 1 : Fiche d'évaluation de la démarche d'homologation d'un projet

[Nom du projet]

Sommaire

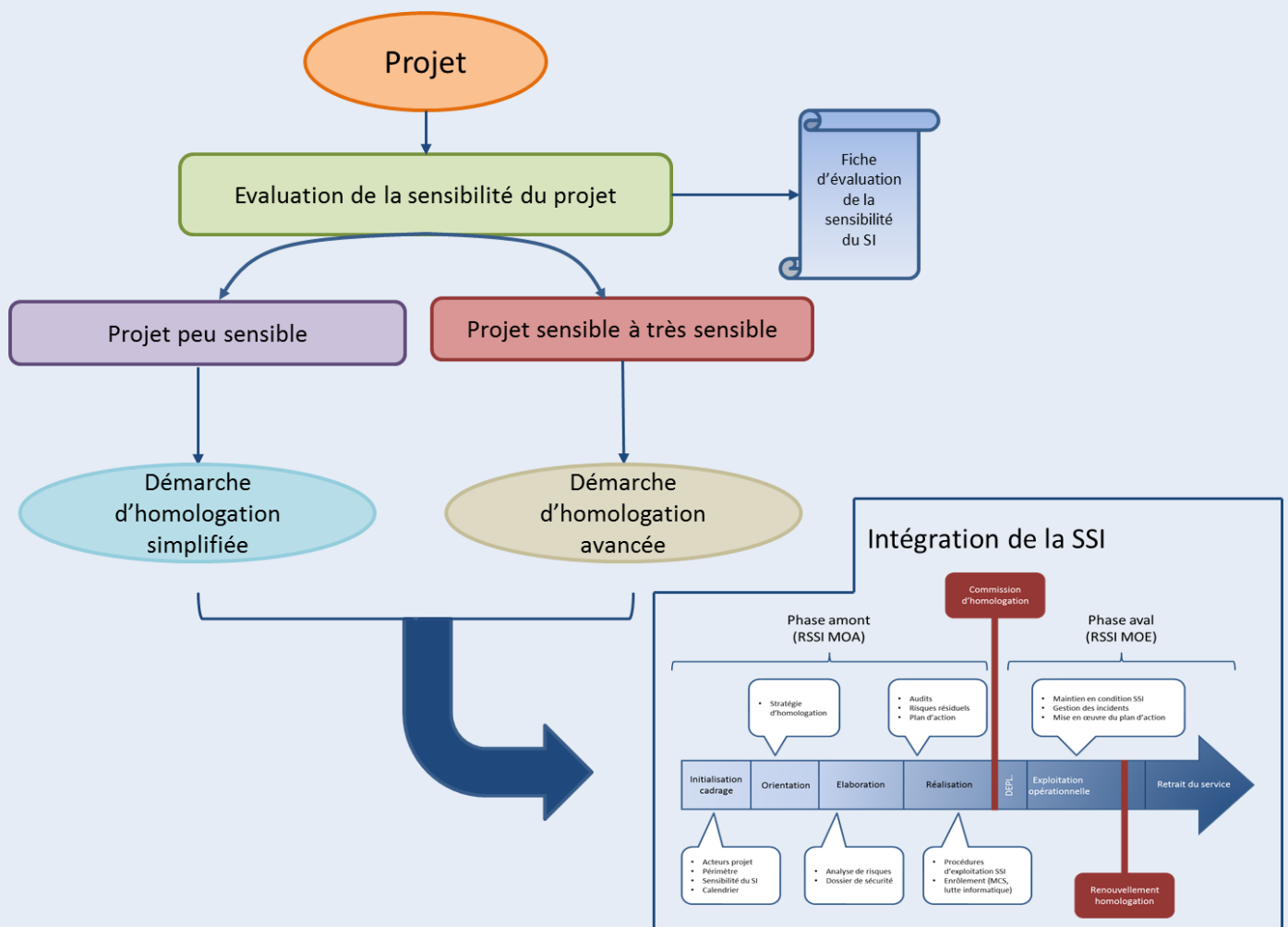
- 1. OBJECTIF DU DOCUMENT 2
- 1. RAPPEL DE LA DEMARCHE D’HOMOLOGATION 2
- 2. QUESTIONNAIRE..... 3
 - 2.1 NIVEAU DE SENSIBILITE A LA SECURITE D’UN PROJET 3
 - 2.2 AMPLEUR DU PROJET..... 7
 - 2.2 CONTROLE DE COHERENCE..... 8
- ANNEXE 1 : ECHELLE DE SENSIBILITE 9

1. OBJECTIF DU DOCUMENT

Ce document est à compléter par tous les chefs de projets en charge d'un nouveau projet ou d'une mise à jour substantielle d'un projet pouvant avoir un impact sur le niveau de sécurité, en interrogeant si besoin les acteurs impliqués (ex : maîtrise d'ouvrage, spécialistes et partenaires du Ministère). L'utilisation de ce questionnaire s'inscrit dans la démarche d'homologation.

2. RAPPEL DE LA DEMARCHE D'HOMOLOGATION

La démarche est adaptée à la sensibilité du projet, qui peut être examinée sur la base du questionnaire figurant dans la présente fiche.



3. QUESTIONNAIRE

3.1 Niveau de sensibilité à la sécurité d'un projet

Le niveau de sensibilité à la sécurité d'un projet informatique s'évalue en sélectionnant les réponses les plus ajustées du questionnaire ci-dessous.

A titre d'exemple, les réponses proposées pour un projet de mise en place d'un site WEB sont indiquées à la suite de chaque question.

Question 1 : Votre système est important pour remplir vos missions ?

| | | |
|--------------------------|--|-----|
| <input type="checkbox"/> | Oui, les missions dépendent totalement du SI | +10 |
| <input type="checkbox"/> | Oui, les missions seraient fortement perturbées en cas de dysfonctionnement | +5 |
| <input type="checkbox"/> | Oui, les missions seraient légèrement perturbées en cas de dysfonctionnement | +3 |
| <input type="checkbox"/> | Non | +0 |

Le projet de site web est un portail d'accès à plusieurs applications métiers. Les missions seraient fortement perturbées en cas de dysfonctionnement (+5 à la note de sensibilité).

Question 2 : quels sont les besoins « métier » en terme de disponibilité du produit du projet ?

La disponibilité est la propriété d'accessibilité au moment voulu des éléments du projet par les utilisateurs autorisés. Certaines ressources ne peuvent pas se trouver inaccessibles sans avoir des répercussions graves sur le Ministère.

| | | |
|--------------------------|----------------------------------|-----|
| <input type="checkbox"/> | Importante (sans délai) | +10 |
| <input type="checkbox"/> | Moyenne (dans la journée) | +5 |
| <input type="checkbox"/> | Faible (sous quelques jours) | +3 |
| <input type="checkbox"/> | Très faible (plusieurs semaines) | +0 |

Projet site WEB : sa disponibilité est importante (+10 à la note de sensibilité).

Question 3 : le projet met-il en œuvre l'utilisation de données à protéger ?

La classification des données est réalisée à l'aide de l'annexe 1 de la présente.

| | | |
|--------------------------|-----------------|-----|
| <input type="checkbox"/> | Secrètes | +10 |
| <input type="checkbox"/> | Confidentielles | +5 |
| <input type="checkbox"/> | Restreintes | +2 |
| <input type="checkbox"/> | Publiques | +0 |

Projet site WEB : les données exposées sont consultables depuis Internet et sont publiques (+0 à la note de sensibilité).

Question 4 : quels sont les besoins métier en terme d'intégrité (cf. 4. échelle de sensibilité) du produit du projet ?

L'intégrité est la propriété d'exactitude et de complétude des éléments du projet. Par exemple la perte d'intégrité d'un document peut être entraînée par erreur (saisie de données d'entrée d'une application fausses...) ou par malveillance (altération volontaire de documents papier, envoi de mail en usurpant l'identité de l'émetteur...). Le non- respect de l'intégrité de certains éléments peut avoir des conséquences néfastes sur le Ministère.

| | | |
|--------------------------|---------------------------|-----|
| <input type="checkbox"/> | Intégrité totale | +10 |
| <input type="checkbox"/> | Intégrité corrigible | +5 |
| <input type="checkbox"/> | Intégrité vérifiable | +2 |
| <input type="checkbox"/> | Faible besoin d'intégrité | +0 |

Projet site WEB : si l'application est modifiée, il peut y avoir une conséquence négative sur l'image de marque du Ministère. L'intégrité est donc importante (+10 à la note de sensibilité)

Question 5 : quels sont les besoins métier en terme de traçabilité (cf. 4. échelle de sensibilité) du produit du projet ?

La **traçabilité** désigne la situation permettant de disposer de l'information **nécessaire et suffisante** pour connaître (éventuellement de façon rétrospective) les opérations réalisées sur un système ou sur une donnée. L'absence ou la perte de traçabilité de certains éléments peut avoir des impacts significatifs sur le Ministère.

| | | |
|--------------------------|------------------------------------|-----|
| <input type="checkbox"/> | Besoin de traçabilité légale | +10 |
| <input type="checkbox"/> | Besoin de traçabilité systématique | +5 |
| <input type="checkbox"/> | Besoin pour information | +2 |
| <input type="checkbox"/> | Faible ou nul | +0 |

Projet site WEB : si le serveur hébergeant l'application est attaqué, il sera nécessaire de disposer des preuves de connexion au système pour prouver l'action malveillante. L'intégrité est donc importante (+10 à la note de traçabilité).

Question 6 : le projet est-il soumis à des contraintes réglementaires, législatives particulières ?

| | | |
|--------------------------|--|----|
| <input type="checkbox"/> | Contraintes règlementaires « métier » à intégrer | +2 |
| <input type="checkbox"/> | ... | |
| <input type="checkbox"/> | Règlement général sur la protection des données | +2 |

Projet site WEB : les règlements donnés en amont ne concernent pas le projet : aucune case n'est cochée (+0 à la note de sensibilité).

Si d'autres règlements spécifiques au projet existent et bien qu'ils ne soient spécifiés en amont, il convient d'ajouter +2 à la note de sensibilité.

Dans tous les cas, il faut respecter les lois (LCEN, Loi Godfrain...) tout au long de l'existence du site WEB.

Question 7 : quelle est la portée du projet en terme d'objectifs métiers (selon la maîtrise d'ouvrage) pour le Ministère (clients du projet) ?

| | | |
|--------------------------|---|----|
| <input type="checkbox"/> | L'application est nationale et diffusée dans le Ministère | +5 |
| <input type="checkbox"/> | L'application est nationale et utilisée par l'Administration Centrale | +2 |
| <input type="checkbox"/> | L'application est nationale et utilisée par les Directions Régionales | +2 |
| <input type="checkbox"/> | L'application est nationale et utilisée par les Directions Départementales | +2 |
| <input type="checkbox"/> | L'application est nationale et utilisée par les partenaires du Ministère | +2 |
| <input type="checkbox"/> | L'application est nationale et utilisée à l'extérieur (entreprises, public) | +2 |
| <input type="checkbox"/> | L'application est locale est destinée à une ou deux directions ou régions | +3 |

Projet site WEB : les données mises à disposition sur le serveur sont des informations concernant tout le Ministère mais pas d'autres partenaires. L'objectif métier concerne le Ministère dans sa totalité (+5 à la note de sensibilité).

Question 8 : quelle est la portée technique (selon la maîtrise d'œuvre) du projet en terme d'utilisation des ressources du SI du Ministère ?

| | | |
|--------------------------|--|-----|
| <input type="checkbox"/> | L'application a une portée technique nationale (ex : utilisation de nombreuses ressources (serveurs, applications, bases de données... du SI du Ministère) | +10 |
| <input type="checkbox"/> | L'application a une portée IT régionale (ex : utilisation d'un réseau régional) | +5 |
| <input type="checkbox"/> | L'application a une portée technique locale (ex : utilisation d'un réseau local propre au projet et de peu de ressources du SI du Ministère) | +1 |

Projet site WEB : l'application utilise un serveur et les équipements du Ministère pour la connexion sur Internet. L'application est locale (+1 à la note de sensibilité).

Question 9 : le projet est adressé à :

| | | |
|--------------------------|---------------------------|-----|
| <input type="checkbox"/> | plus de 3000 utilisateurs | +10 |
| <input type="checkbox"/> | plus de 1000 utilisateurs | +5 |
| <input type="checkbox"/> | plus de 500 utilisateurs | +3 |
| <input type="checkbox"/> | moins de 500 utilisateurs | +1 |

Projet site WEB : s'adresse à plus de 3000 utilisateurs (+10 à la note de sensibilité).

Question 10 : les technologies qui seront utilisées par le projet sont :

| | | |
|--------------------------|--|----|
| <input type="checkbox"/> | très diverses (divers outils de développement, systèmes d'exploitation et utilitaires, protocoles réseau, fournisseurs d'équipements et accès...) impliquant un besoin de compétences pointues | +3 |
| <input type="checkbox"/> | nouvelles sur les marchés et encore peu développées | +3 |
| <input type="checkbox"/> | peu connues et maîtrisées au sein du Ministère | +3 |

Projet site WEB : une seule application qui offre quelques services en ligne (consultation, transfert de fichiers éventuellement...). Le serveur est intégré aux architectures réseau déjà existantes au Ministère. Aucune case n'est cochée (+0 à la note de sensibilité).

| | |
|----------------------------|--|
| TOTAL DES QUESTIONS | |
|----------------------------|--|

Projet site WEB : la note finale est de 41.

| TOTAL | SENSIBILITE A LA SECURITE DU PROJET |
|-----------------|--|
| 35 > TOTAL | Niveau 1 : peu sensible |
| 60 > TOTAL ≥ 35 | Niveau 2 : sensible |
| TOTAL ≥ 60 | Niveau 3 : très sensible |

Projet site WEB : le niveau de sensibilité du projet est 2.

3.2 Ampleur du projet

Question 1 : le budget réservé au projet est :

| | | |
|--------------------------|--------------------------------|-----|
| <input type="checkbox"/> | Supérieur à 750 000 euros | +10 |
| <input type="checkbox"/> | Entre 150 000 et 750 000 euros | +5 |
| <input type="checkbox"/> | Entre 90 000 et 150 000 euros | +3 |
| <input type="checkbox"/> | Inférieur à 90 000 euros | +1 |

Projet site WEB : le budget est entre 90 000 et 150 000 euros (+3 à la note d'ampleur).

Question 2 : le projet est à réaliser sur une période de :

| | | |
|--------------------------|--------------------------|-----|
| <input type="checkbox"/> | Plus de deux ans | +10 |
| <input type="checkbox"/> | Entre un et deux ans | +5 |
| <input type="checkbox"/> | Entre deux mois et un an | +3 |
| <input type="checkbox"/> | Moins de deux mois | +1 |

Projet site WEB : le projet est à réaliser sur une période entre deux mois et un an (+3 à la note d'ampleur).

TOTAL DES QUESTIONS

Projet site WEB : la note d'ampleur est de 6.

| TOTAL | AMPLEUR DU PROJET |
|----------------|-------------------|
| TOTAL = 20 | Niveau 1 |
| 20 > TOTAL ≥ 5 | Niveau 2 |
| 5 > TOTAL | Niveau 3 |

Projet serveur WEB : le niveau d'ampleur est 2.

3.3 Contrôle de cohérence

| | | SENSIBILITE A LA SECURITE | | |
|-------------------------|----------|--|--|--|
| | | Niveau 1 | Niveau 2 | Niveau 3 |
| AMPLEUR DU PROJET | Niveau 1 | Les ressources associées au projet sont en cohérence avec le niveau de sensibilité | Les ressources associées au projet sont en cohérence avec le niveau de sensibilité | Les ressources associées au projet sont en cohérence avec le niveau de sensibilité |
| | Niveau 2 | Les ressources associées au projet sont en cohérence avec le niveau de sensibilité | Les ressources associées au projet sont en cohérence avec le niveau de sensibilité | Les ressources associées au projet ne sont pas en cohérence avec le niveau de sensibilité |
| | Niveau 3 | Les ressources associées au projet sont en cohérence avec le niveau de sensibilité | Les ressources associées au projet ne sont pas en cohérence avec le niveau de sensibilité | Les ressources associées au projet ne sont pas en cohérence avec le niveau de sensibilité |

Si le projet se trouve dans un état de non cohérence entre les ressources disponibles en terme de budget et de temps, et son niveau de sensibilité, il convient de réévaluer les ressources jusqu'à l'obtention d'un état de cohérence approprié. Un projet se trouvant en état de non cohérence met en danger des ressources du SI du Ministère, car les risques pesant sur ces actifs ne pourront être réduits. En effet des délais trop courts ou des budgets limités ne pourront pas permettre la mise en œuvre de mesures de sécurité dans les phases aval du projet, alors qu'elles seront certainement nécessaires vu le niveau de sensibilité du projet.

Projet site WEB : le niveau d'ampleur et de sensibilité étant de 2, on peut considérer que les ressources associées au projet sont en cohérence avec le niveau de sensibilité.

4 ECHELLE DE SENSIBILITE

| Confidentialité | | | |
|--|---|---|---|
| 0 Public | 1 Restreint | 2 Confidentiel | 3 Secret |
| <i>L'élément essentiel peut être rendu public</i> | <i>L'accès à l'élément essentiel est restreint aux personnels ou process internes autorisés de par leur fonction ou de par leur appartenance à un entité organisationnelle.</i> | <i>L'accès à l'élément essentiel est restreint aux personnels ou process internes autorisés de par leur fonction ou de par leur appartenance à un entité organisationnelle, et qui par ailleurs ont le besoin d'en connaître.</i> | <i>Accès strictement restreint aux seuls personnels nommément désignés par la loi ou un règlement.</i> |
| Disponibilité | | | |
| 0 Très faible | 1 Faible | 2 Moyenne | 3 Importante |
| <i>L'élément essentiel peut être indisponible pour une longue période.</i> | <i>L'élément essentiel doit être disponible sous quelques jours.</i> | <i>L'élément essentiel doit être disponible dans la journée, aux personnes qui ont le besoin d'en disposer</i> | <i>L'élément essentiel doit être disponible sans délai, aux personnes qui ont le besoin d'en disposer.</i> |
| Intégrité | | | |
| 0 Faible | 1 Intégrité vérifiable | 2 Intégrité corrigible | 3 Intégrité totale |
| <i>L'élément essentiel peut ne pas être intègre.</i> | <i>Besoin de détection du caractère intègre ou non-intègre de l'élément essentiel, sans correction nécessaire.</i> | <i>Besoin de détection du caractère intègre ou non intègre de l'élément essentiel, avec correction requise si besoin.</i> | <i>L'intégrité de l'élément essentiel doit être totale aussi bien pendant sa période d'utilisation qu'ultérieurement (Ex: archivage légal ou opérationnel).</i> |
| Traçabilité | | | |
| 0 Faible ou nul | 1 Besoin pour information | 2 Besoin de traçabilité systématique | 3 Traçabilité légale |
| <i>Aucun besoin de traçabilité.</i> | <i>Besoin de traçabilité pour information, avec enregistrement éventuel d'une trace (non nécessairement détaillée).</i> | <i>Besoin de traçabilité pour information, avec enregistrement systématique d'une trace détaillée (Exemple, besoin commercial ou de facturation).</i> | <i>Besoin légal de traçabilité avec enregistrement systématique de trace comme élément de preuve indiscutable.</i> |

Annexe 2 : Stratégie d'homologation type

[Nom du projet]

Sommaire

| | | |
|-----------|--|-----------|
| 1. | OBJECTIF DU DOCUMENT..... | 12 |
| 2. | PRESENTATION | 12 |
| 3. | ACTEURS ET RESPONSABILITES..... | 14 |
| 4 | DOSSIER D'HOMOLOGATION | 17 |
| 5 | PROCESSUS D'HOMOLOGATION..... | 19 |

1. OBJECTIF DU DOCUMENT

Ce document a pour objet de définir la stratégie d'homologation du système [XXX] dans le cadre des exigences du Référentiel Général de Sécurité (RGS)

L'homologation de sécurité, prononcée par l'autorité qualifiée après avis d'une commission ad hoc, atteste de la capacité d'un système à traiter des informations sensibles au vu des mesures qu'il met en œuvre pour les protéger. Elle traduit l'acceptation d'un niveau quantifié de risques résiduels pour la confidentialité, l'intégrité et la disponibilité.

La présente stratégie d'homologation a pour objectif de présenter les étapes et les éléments nécessaires à l'homologation de sécurité du système [XXX]. Elle comporte notamment :

- la définition du périmètre faisant l'objet de l'évaluation ;
- les méthodes et référentiels retenus ;
- la liste des documents de sécurité (dossier d'homologation) et outils qui permettront d'analyser et de maîtriser les risques de sécurité ;
- le dossier d'architecture technique.

2. PRESENTATION

2.1 Contexte d'emploi

i. Contexte général

Décrire le contexte de mise en œuvre du système.

Le système [XXX] est composé, pour le Ministère de la justice :

ii. 2.1.2 Identification des parties prenantes

Acteurs : il s'agit des parties prenantes garant de la conception (maitre d'ouvrage) puis de l'exploitation du système [XXX]

Fournisseurs : il s'agit des contributeurs à la conception, au déploiement et à l'exploitation du système [XXX]

(Prestataires : hébergeurs)

Clients : il s'agit des utilisateurs du système [XXX] :

agents de la justice (en centrale et en services déconcentrés)

Partenaires : il s'agit des entités disposant d'un réseau propre et d'un raccordement spécifique au système [XXX] :

- agents de la justice (services décentralisés)

- Partenaires externes à l'administration

- Ministères

2.2 Limites du périmètre d'homologation

L'homologation concerne les services fournis par le MinJU ainsi que les processus nécessaires au fonctionnement du système [XXX] à destination de ses partenaires : exploitation, administration, supervision, gestion de la sécurité, gestion administrative et contractuelle, évolution technique et gouvernance.

Le périmètre fonctionnel et technique à considérer comprendra :

- l'application [XXX] ;

- le service [XXX] ;

- la plateforme [XXX].

L'homologation du système se limitera dans un premier temps au périmètre constitué de :

- [XXX]

3. ACTEURS ET RESPONSABILITES

3.1 Autorité d'homologation

L'autorité responsable de l'homologation du système [XXX] est la secrétaire générale du ministère de la justice. Cette fonction ne peut être déléguée. Elle est chargée d'approuver la démarche d'homologation et le dossier d'homologation basé notamment sur :

- la prise en compte des exigences de sécurité et des risques résiduels identifiés (cf. Analyse de risques) ;
- le suivi et la validation du dossier d'homologation à travers de réunions régulières.

Elle s'appuie sur la commission d'homologation, dont elle fixe la composition. La désignation de ces membres pourra être subordonnée, si besoin, à leur habilitation préalable au niveau nécessaire.

Elle veille à ce que tous les acteurs concourant à la sécurité du système d'information soient identifiés, désignés et habilités.

Ces missions incluent en particulier :

- examiner et approuver les rapports d'homologation ;
- approuver la décision d'homologation du système [XXX] ;
- émettre le certificat d'homologation du système [XXX].

Selon les résultats de l'analyse de risques effectuée dans le cadre de la démarche d'homologation, l'autorité d'homologation pourra prononcer :

- une homologation provisoire (ou autorisation provisoire d'emploi), assortie de réserves et d'un délai de mise en conformité des défauts de sécurité rencontrés ;
- une homologation pour une durée déterminée ;
- un refus d'homologation, si les risques résiduels sont jugés inacceptables.

3.2 Autorité d'emploi

L'autorité d'emploi du système est [XXX] du ministère de la justice. Elle assure également les fonctions de maîtrise d'ouvrage (MOA) et de direction de l'exploitation des briques applicatives et d'échanges de données. Il est chargé de :

- s'assurer du fonctionnement des briques visées au paragraphe 2.2 ;
- gérer la bonne utilisation des moyens, tant humains que techniques, nécessaires à son fonctionnement ;
- contrôler l'application des mesures de sécurité préconisées ;
- proposer les évolutions nécessaires au regard des contraintes d'emploi ou de l'évolution fonctionnelle des besoins ;
- diligenter au besoin les audits de sécurité.

3.3 Commission d'homologation

Pour mener à bien sa mission, l'autorité d'homologation s'appuie sur l'avis organisationnel et technique fourni par la commission d'homologation. Elle est donc chargée de fournir un avis motivé sur la capacité du système à répondre ou non aux objectifs de sécurité assignés, de s'assurer que l'ensemble des mesures techniques et organisationnelles permettant la sécurisation du système ont toutes été prises et sont correctement appliquées.

Pour cela, elle est chargée de :

- rédiger, revoir et maintenir la stratégie d'homologation du système [XXX] ;
- suivre la constitution du dossier d'homologation ;
- examiner et analyser toutes les preuves de sécurité requises pour l'homologation ;
- diligenter au besoin les audits de sécurité ;
- examiner et proposer le besoin en termes de post-homologation et ré-homologation.

La commission d'homologation est présidée par l'autorité d'homologation. Le secrétariat et l'organisation sont confiés à [XXX]. L'autorité d'homologation prend les décisions après consultation et avis des membres de la commission d'homologation.

La commission d'homologation de sécurité est composée comme suit :

[Homologation simple]

■ Membres permanents :

- Autorité d'homologation (à préciser) ;
- le chef ou le directeur de projet MOA ;
- les RSSI du métier (à préciser) et de la DSI (SSIC) ;
- le FSSI ou son représentant.

■ Invités (si nécessaire) :

- les auditeurs et/ou experts techniques, notamment dans le domaine de la SSI ;
- l'AQSSI ou son représentant.

[Homologation avancée]

| Pour les applications métiers | Pour les services transverses offerts par le SSIC |
|---|---|
| <h5>■ Membres permanents :</h5> <ul style="list-style-type: none"> - Autorité d'homologation (à préciser) ; - le chef ou le directeur de projet MOA ; - Responsables des applications métiers (à préciser) ; - les AQSSI concernées (à préciser) ; - les RSSI du métier (à préciser) et de la DSI (SSIC) ; - le FSSI (ou son représentant). <h5>■ Invités (si nécessaire) :</h5> <ul style="list-style-type: none"> - les auditeurs et/ou experts techniques, notamment dans le domaine de la SSI. | <h5>■ Membres permanents :</h5> <ul style="list-style-type: none"> - Autorité d'homologation (SSIC) ; - le chef ou le directeur de projet MOA ; - Responsables des services transverses (à préciser) ; - Représentants des directions utilisatrices ; - les AQSSI concernées (à préciser) ; - les RSSI du métier (à préciser) et de la DSI (SSIC) ; - le FSSI (ou son représentant). <h5>■ Invités (si nécessaire) :</h5> <ul style="list-style-type: none"> - les auditeurs et/ou experts techniques, notamment dans le domaine de la SSI. |

3.4 Comité de gestion des risques

Ce groupe instruit l'ensemble des questions relatives à la sécurité du système. Il élabore un ensemble de propositions qu'il transmet à la commission d'homologation. Il a notamment pour mission de réaliser ou faire réaliser :

- les analyses de risques ;
- les audits de sécurité ;
- le suivi des plans d'action ;
- le dossier de sécurité.

Ce groupe est constitué comme suit :

■ Membres permanents :

- Le chef ou le directeur de projet MOA ;
- Les représentants des chaînes SSI du ministère de la justice (métiers et SSIC) impliqués dans le projet (à préciser) ;

■ Invités (si nécessaire) :

- les auditeurs et/ou experts techniques, notamment dans le domaine de la SSI ;
- les responsables d'exploitation ;
- le représentant des industriels assurant la tierce maintenance applicative du système.

Le comité de gestion des risques se réunira autant que de besoin (a minima semestriellement, a maxima trimestriellement) pour réaliser les tâches qui lui incombent.

3.5 Responsables de la SSI du système

Pour chacune des briques composant le système [XXX] à la justice, la décision d'homologation relève de l'autorité qualifiée en matière de défense et de sécurité.

La liste des autorités qualifiées figure ci-dessous :

- AQSSI XXX ;
- AQSSI XXX.

Le pilotage de la sécurité du système [XXX] est répartie sur la chaîne fonctionnelle SSI et en particulier sur :

- les RSSI métiers qui spécifient les besoins ;
- les RSSI du SSIC.

Les RSSI s'assureront, sur le périmètre dont ils ont la responsabilité, du respect de l'application des mesures de sécurité.

3.6 Qualification et audits

Le directeur de projet peut diligenter ou faire diligenter à tout moment des audits de sécurité. Ces audits seront régulièrement menés afin de vérifier la bonne application de règles de sécurité sur l'ensemble du périmètre d'homologation. Un audit de sécurité sera par ailleurs systématiquement effectué après tout incident révélant une défaillance dans l'application des règles de sécurité.

Un audit de sécurité fera systématiquement l'objet d'un compte rendu, pouvant être assorti de mesures correctives à appliquer et d'un calendrier de mise en conformité. Un audit de vérification pourra être effectué pour contrôler cette mise en conformité.

4. DOSSIER D'HOMOLOGATION

Le dossier d'homologation des briques composant le système [XXX] de la justice est considéré de niveau [X], conformément à la PMDS.

Le dossier d'homologation comportera les pièces suivantes :

[Homologation simple]

- la stratégie d'homologation ;
- l'analyse de risques macroscopique ;
- la synthèse des tests et des audits menés pour s'assurer de la robustesse du système face aux enjeux de sécurité ;
- le plan de remédiation ;
- (si besoin) les décisions d'homologation des SI interconnectés.

[Homologation avancée]

- la stratégie d'homologation ;
- l'analyse de risques ;
- la politique de sécurité du système d'information ;
- le dossier d'architecture technique ;
- les procédures d'exploitation de la sécurité ;
- les rapports d'audits ;
- le document de traitement des risques résiduels
- pour les moyens de chiffrement et produits de sécurité :
 - o la description des mécanismes de sécurité spécifiques ;
 - o le certificat de qualification émis par l'ANSSI ;
 - o les rapports éventuels de certification ITSEC ou Critères Communs.

4.1 Stratégie d'homologation

Il s'agit du présent document.

4.2 Analyse de risques

Une analyse de risques macroscopique sera produite avant la mise ne œuvre de l'expérimentation. Elle permettra de synthétiser les principaux risques métiers et techniques. Elle s'appuiera sur la réalisation d'audits pour mettre en exergue les vulnérabilités résiduelles en présence et le plan de remédiation à conduire.

Une analyse de risque doit être conduite, sous la responsabilité des maîtrises d'ouvrages, (en s'appuyant sur la méthodologie EBIOS) pour chacune des briques constituant de système d'information. Elle décrit formellement les objectifs de sécurité en matière de disponibilité, d'intégrité, de confidentialité et de traçabilité dans le contexte d'un ensemble de menaces identifiées.

Ces analyses de risques déclineront les exigences de sécurité qui doivent être prises en compte par le système [XXX].

4.3 Politique de sécurité du système d'information

La politique de sécurité du système [XXX] décrit l'ensemble de mesures de sécurité à mettre en œuvre pour respecter les conditions d'emploi et maintenir son niveau de sécurité. Il s'agira en l'espèce de faire la synthèse des PSSI des briques techniques composant le système [XXX].

Tout aménagement à cette politique doit faire l'objet d'une étude d'impact en termes de sécurité et l'acceptation doit faire l'objet d'un accord explicite du directeur de projet.

4.4 Dossier d'architecture technique

Le dossier d'architecture présente l'architecture technique des composantes du système [XXX] et précise les obligations, recommandations ou éventuelles contraintes à leur maintien en condition opérationnelle ou de sécurité. Il inclut les contraintes d'installation applicables pour le déploiement des services spécifiques aux partenaires. Il décrit les prérequis nécessaires à son déploiement, son architecture et sa mise en œuvre sur les différents sites.

4.5 Procédure d'exploitation de la sécurité

Ce document expose les procédures d'exploitation de sécurité du Ministère de la justice en relation avec les procédures d'exploitation de sécurité des différents partenaires (services centraux du ministère de la justice, juridictions et services déconcentrés, [XXX]). Ce document est la déclinaison opérationnelle des mesures établies dans la PSSI.

4.6 Rapports d'audits de sécurité

Les contrôles de sécurité feront apparaître :

- les vulnérabilités qui n'auraient pas été prises en compte dans l'analyse de risques initiale ;
- l'évolution de l'état de la menace ;
- la découverte de nouvelles vulnérabilités ;
- la préconisation des mesures correctrices.

La mise en œuvre des audits doit s'opérer à fréquence régulière.

[Remarque : si le système à homologuer est interconnecté à d'autres systèmes non-homologués, il est fortement recommandé de demander aux maitrises d'ouvrages dont ces systèmes dépendent de réaliser des audits (en priorité audit de configuration et tests d'intrusion). Les résultats permettront ainsi d'évaluer les vulnérabilités auxquels ces systèmes sont exposés et permettre à l'autorité d'homologation de prendre une décision quant à la mise en production du système considéré.]

4.7 Plan d'action (plan de remédiation)

Ce document établit un plan d'action ("action plan"), avec des objectifs temps et résultat, accompagné de la mise sur pied d'un groupe de personnes aptes à le mettre en œuvre ("task force"), aux fins de remédier à des situations insatisfaisantes dans l'organisation ou le respect des normes ("compliance") dans le domaine de la sécurité.

4.8 Synthèse des risques résiduels

Il s'agit ici de synthétiser les risques résiduels qui devront être acceptés par l'autorité d'homologation.

5. PROCESSUS D'HOMOLOGATION

5.1 Principe général

Conformément à l'article 14 de l'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, les autorités administratives doivent mettre leurs systèmes d'information existants à la date de publication du RGS en conformité avec ce référentiel dans un délai de trois ans à compter de sa publication. Les systèmes créés dans les six mois qui suivent la publication du RGS doivent être mis en conformité dans un délai de 12 mois. Cette conformité est un préalable à la mise en service opérationnelle de tout système d'information. Par ailleurs, le Référentiel Général de Sécurité (RGS) impose aux autorités administratives d'homologuer les systèmes d'informations permettant l'échange d'informations entre autorités différentes. En tant qu'infrastructure interministérielle, le programme « procédures pénales numériques » relève du RGS et doit donc être homologué.

L'homologation est l'acte selon lequel l'autorité atteste formellement auprès des utilisateurs que le système d'information est protégé conformément aux objectifs de sécurité fixés. La décision d'homologation est prise par l'autorité d'homologation (désignée par l'autorité qualifiée) après avis, le cas échéant, de la commission d'homologation. Cette décision précise les conditions d'emploi du système d'information considéré.

5.2 Stratégie d'homologation

L'homologation du système [XXX] est conditionnée par [à compléter].

5.3 Durée d'homologation

L'homologation initiale est demandée pour une durée de xx Mois/an. Durant cette période, l'homologation pourra être revue selon les modalités et principes exposés ci-après.

5.4 Révision de l'homologation

Une révision de l'homologation est nécessaire à l'issue de cette période ou si un fait significatif de nature à remettre en cause l'homologation en cours, dont le périmètre du système a été précisé, est constaté. La liste ci-après énumère un certain nombre d'événements qui impliquent le renouvellement de l'homologation :

- modifications majeures de l'architecture du réseau ou introduction d'une interconnexion non prévue ;
- modifications majeures des composants du réseau (matériels, configuration logicielle, etc.) ;
- modification du niveau de menace portant sur le système considéré ;
- changement de classification de l'information traitée ;
- incident de sécurité qui remet manifestement en cause l'homologation en cours ;
- résultats non satisfaisants d'une inspection, contrôle ou audit de sécurité ;
- fin de la période initiale d'homologation ;
- plus généralement, sur décision de l'autorité d'homologation.

5.5 Suivi de l'homologation

L'homologation d'un système d'information est non seulement l'un des objectifs à atteindre avant sa mise en service, mais également l'attestation d'un état de protection dont il faudra garantir le maintien jusqu'à la décision du retrait de service. La procédure mise en œuvre pour l'homologation d'un système doit donc revêtir un caractère itératif tout au long du cycle de vie de ce système.

Afin d'avoir une vision dans le temps du niveau de sécurité des systèmes et applications homologués, la commission d'homologation se réunit a minima une fois par an afin d'examiner les points suivants :

- suivi des indicateurs de sécurité du réseau, pouvant inclure des indicateurs d'exploitation. Ces indicateurs de niveau stratégique, pilotage et opérationnel seront définis par le comité de gestion des risques, validés par la commission d'homologation et inscrit dans la PSSI ;
- analyse des retours sur incidents SSI éventuels ;
- information sur les évolutions du réseau ou des systèmes d'information ministériels pouvant impacter sur l'homologation ;
- réévaluation éventuelle de la menace ou des objectifs de sécurité induisant une mise à jour de l'analyse de risques et des mesures de sécurité mises en œuvre.

La commission d'homologation peut se réunir de manière exceptionnelle ou à une fréquence plus régulière sur demande justifiée au Président de la commission de l'un de ses membres ou du comité de gestion des risques. La révision de l'homologation, pour l'un des motifs précédemment cités, ou un risque SSI particulier peuvent justifier d'une réunion exceptionnelle.

Annexe 3 : Procédure de gestion des risques

[Nom du projet]

Sommaire

| | | |
|----------|---|-----------|
| 1 | OBJECTIFS | 23 |
| 2 | VOCABULAIRE ET DEFINITION DES RISQUES ET DE LA GESTION DES RISQUES | 23 |
| 3 | RESPONSABILITES | 24 |
| 4 | OUTILLAGES | 25 |
| 4.1 | CENTRALISATION DES RISQUES | 25 |
| 4.2 | MODELE DE PRESENTATION DES RISQUES | 25 |
| 5 | DEROULEMENT DE LA PROCEDURE DE GESTION DES RISQUES | 25 |
| 5.1 | A. APPRECIATION ET PROPOSITION DE TRAITEMENT DES RISQUES | 26 |
| 5.1.1 | <i>Etape a1 : Identification des scénarios de risques</i> | <i>27</i> |
| 5.1.2 | <i>Etape a2 : Estimation & évaluation des risques</i> | <i>28</i> |
| 5.1.3 | <i>Etape a3 : Définition du traitement</i> | <i>30</i> |
| 5.1.4 | <i>Etape a4 : Mise à jour du suivi des risques</i> | <i>31</i> |
| 5.2 | ACTIVITE B SUIVI DU TRAITEMENT DES RISQUES SSI | 31 |
| 5.2.1 | <i>Etape b1 : Suivi des risques et de leur traitement</i> | <i>32</i> |
| 5.2.2 | <i>Etape b2 : Présentation au Comité de gestion des risques</i> | <i>32</i> |
| 5.2.3 | <i>Etape b3 : Arbitrage par le Comité de gestion des risques</i> | <i>32</i> |
| 5.2.4 | <i>Etape b4 : Définition d'un plan projet</i> | <i>33</i> |
| 5.2.5 | <i>Etape b5 : Mise à jour du suivi des risques</i> | <i>33</i> |
| 6 | SURVEILLANCE ET REVUE DES RISQUES | 33 |
| 6.1 | REVUE ANNUELLE COMPLETE DES RISQUES | 33 |
| 6.2 | SURVEILLANCE ET REVUE DES FACTEURS DE RISQUES | 33 |
| 6.3 | GESTION DES RISQUES DES SERVICES OPERES PAR DES « TIERS » | 34 |
| 7 | REVUE ET AMELIORATION DU PROCESSUS DE GESTION DES RISQUES | 35 |
| 8 | ANNEXES | 36 |
| 8.1 | DIFFERENTS ETATS D'UN RISQUE | 36 |
| 8.2 | CONVENTION POUR LES REFERENCES DE RISQUES | 37 |
| 8.3 | COMPLEXITE DE MISE EN ŒUVRE | 37 |
| 8.4 | AIGUILLAGE TRAITEMENT DES RISQUES | 40 |
| 8.5 | INDICATEURS DU PROCESS DE GESTION DES RISQUES | 41 |

1 OBJECTIFS

Cette procédure a vocation à définir les principes de la **gestion des risques numériques** au sein du ministère de la justice (identification, évaluation, proposition d'un plan de traitement, arbitrage par la MOA, suivi).

La gestion des risques numériques doit permettre à une organisation **d'identifier les risques pesant sur ses activités** et de se positionner vis-à-vis de ces risques soit en les acceptant, en les transférant ou en les traitant afin de les amener à un niveau qu'elle puisse juger acceptable.

La mise en œuvre d'une procédure de gestion des risques numériques permet au ministère de la justice :

- de se mettre en conformité avec les textes en vigueur en matière de cybersécurité notamment le **Référentiel Général de Sécurité (RGS)**¹ qui implique la mise en œuvre d'une démarche de gestion des risques consistant à :
 - établir le contexte de mise en œuvre du système ;
 - identifier, apprécier et hiérarchiser les risques ;
 - traiter les risques (les réduire ou les éviter, et accepter de prendre les risques résiduels).

Le RGS recommande l'utilisation de la norme ISO/CEI 27005.

- de se mettre en conformité avec l'aspect contrôle de la **norme ISO27001 : 2017** qui prône une approche du contrôle par le risque ;
- de s'assurer qu'elle connaît et comprend les risques auxquels elle s'expose ;
- de dresser et mettre en œuvre un plan destiné à prévenir l'occurrence de ces risques ou à en minimiser l'impact.

2 VOCABULAIRE ET DEFINITION DES RISQUES ET DE LA GESTION DES RISQUES

La norme ISO27005 définit le risque numériques comme « *la potentialité qu'une menace donnée exploite la ou les vulnérabilités d'un élément ou d'un groupe d'éléments constitutif du système d'information concerné et affecte l'organisation concernée* ».

La présente procédure traite de la **gestion des risques numériques** au ministère de la justice, et vise à en faire ressortir les risques majeurs. Un risque considéré comme majeur est un **risque pouvant mettre en péril les activités régaliennes du ministère, engager sa responsabilité pénale ou nuire à son image**.

La norme ISO 27005 définit également les principaux termes liés à la gestion des risques numériques :

- **Actifs primordiaux**² : les actifs primordiaux sont les informations utilisées dans les processus métiers de l'entreprise ou les processus et activités métiers eux même ;
- **Actifs en support** : les actifs en support sont les actifs utilisés par les actifs primordiaux (matériel, logiciel, réseau, personnel, site, ...), et sur lesquels il peut exister des vulnérabilités ;
- **Identification du risque** : processus permettant d'identifier, de lister et de caractériser les risques ;
- **Estimation du risque** : processus permettant d'associer à un risque une probabilité d'occurrence/opportunité et des conséquences sur les processus métiers impactés ;
- **Evaluation du risque** : processus permettant de comparer le risque estimé aux critères d'acceptation, des risques afin de prioriser les actions de traitement ;
- **Impact** : changement pouvant affecter les objectifs initialement affectés à une activité (processus métier) ;
- **Traitement du risque** : Quatre options de traitement du risque sont possibles :
 - **Acceptation du risque** : processus consistant à accepter et assumer les éventuelles pertes liées à la réalisation d'un risque. (également appelé rétention du risque) ;

¹ Les systèmes d'information du ministère de la justice doivent se conformer au RGS.

² Bien essentiels dans EBIOS2010 & *Risk Manager*

- **Refus/Évitement du risque** : éviter un risque consiste à abandonner l'activité engendrant le risque, ou à modifier les conditions dans lesquelles elle est opérée. Il est par exemple possible de déplacer la responsabilité de l'activité concernée vers une autre organisation : le risque et sa couverture sortent ainsi du périmètre de responsabilité du ministère de la justice ;
- **Réduction du risque** : actions prises afin de minimiser la probabilité d'occurrence et/ou les conséquences sur les processus métiers impactés en cas de survenance du risque ;
- **Transfert du risque** : processus permettant de partager les conséquences liées à la réalisation d'un risque avec une tierce partie. Dans le cadre d'un transfert de risque, seule la couverture du risque est partagée.

Un risque peut passer par différents états de son identification à sa clôture, ces différents états sont présentés à l'annexe 8.1.

3 RESPONSABILITES

Responsable du processus de gestion des risques :

Le processus de gestion des risques est placé sous la **responsabilité de la maîtrise d'ouvrage (MOA) principale ou déléguée**:

Le directeur ou chef de projet MOA est responsable de la bonne prise en compte des enjeux de sécurité et en particulier :

- de la définition de la méthode de gestion des risques, des échelles associées et des indicateurs ;
- de la bonne diffusion de la méthode de gestion des risques aux personnes concernées, et s'assure que celles-ci ont été formées ;
- de la définition des plans d'actions dans le cadre du traitement d'un risque, et du suivi de ces plans d'actions ;
- de la traçabilité des décisions prises (choix du traitement du risque, plan d'actions, acceptation de risques résiduels, etc.) ;
- de la gestion documentaire des documents relatifs au processus de gestion des risques et du suivi centralisé des risques ;
- de l'organisation des différentes réunions relatives à la gestion des risques numériques (exemple : comité de gestion des risques, ...) ;
- de la réalisation par l'Autorité Qualifiée de la Sécurité des Systèmes d'Information (AQSSI)³ de l'arbitrage de la solution de traitement pour réduire le niveau de criticité d'un risque majeur, lorsque celle-ci est complexe ;
- de la présentation de l'ensemble des risques numériques, et de l'identification des risques résiduels ;
- de l'identification des risques « bloqués », de proposer des solutions pour les débloquer et de les faire arbitrer par l'AQSSI (si nécessaire).

Responsables d'actions de traitement d'un risque (acteurs opérationnels) :

Pour réduire un risque, un ou plusieurs responsables d'action de traitement sont identifiés. Ils sont responsables de proposer (en collaboration avec l'équipe SSI) une ou plusieurs actions de traitement. Et une fois qu'elles ont été validées, de suivre leur avancement et en rendre compte régulièrement au responsable de la sécurité des systèmes d'information (RSSI) de la MOA.

Comité de gestion des risques (CGR) :

Ce comité réunit les représentants de la MOA et des équipes SSI fonctionnelles et opérationnelles, dont la responsabilité est d'accepter les niveaux de risques résiduels pour les solutions de traitement proposées pour réduire les risques majeurs, arbitrer lorsqu'elle est complexe la solution de traitement pour un risque majeur. Sa responsabilité est également d'arbitrer et d'appuyer la solution retenue pour « débloquer » un risque dont le traitement est « bloqué ».

³ AQSSI : L'autorité qualifiée SSI est responsable de la sécurité des systèmes d'information au sein de sa direction, du service, de l'établissement ou de l'autorité

4 OUTILLAGES

4.1 Centralisation des risques

Afin de réaliser le suivi global des risques numérique au sein du ministère de la justice, un tableau ou outil de suivi doit être mis en place par le RSSI de la MOA ou par une personne dûment désignée par l'Autorité Qualifiée en SSI rattachée à la MOA.

Dans un premier temps, un tableur sous format *Excel* ou *CALC* pourra être utilisé et contenir à minima les 2 volets suivants:

- A. le suivi des risques numériques ;
- B. le suivi des plans de traitement des risques.

4.2 Modèle de présentation des risques

Lors de la présentation des risques numériques en comité de gestion des risques (étape b2 du point 5.2.2), un modèle de présentation au format Powerpoint standard (Présentation - suivi des risques numériques-) doit être utilisé dans la mesure du possible, afin de garantir une certaine cohérence à l'ensemble des restitutions.

5 DEROULEMENT DE LA PROCEDURE DE GESTION DES RISQUES

La démarche de gestion des risques numérique au ministère de la justice est décomposée en 3 activités :

- A. Appréciation et proposition de traitement des risques
 - Etape a1 : Identification des risques numériques
 - Etape a2 : Estimation et évaluation des risques
 - Etape a3 : Définition d'un plan de traitement des risques
 - Etape a4 : Mise à jour du suivi des risques numériques
- B. Suivi du traitement des risques
 - Etape b1 : Suivi des risques et de leur traitement
 - Etape b2 : Présentation au comité de gestion des risques
 - Etape b3 : arbitrage par le comité de gestion des risques
 - Etape b4 : définition d'un plan projet de traitement des risques
 - Etape b5 : Mise à jour du suivi des risques numériques

L'appréciation des risques, le traitement des risques et l'arbitrage requièrent en outre une **communication régulière sur les risques** de la part du RSSI de la MOA, avec les acteurs opérationnels et les instances de décision.

La communication se fait également au travers des réunions portant sur les risques numériques (comité de gestion des risques) et des rapports annuels réalisés auprès de la cellule HFDS.

5.1 A. Appréciation et proposition de traitement des risques

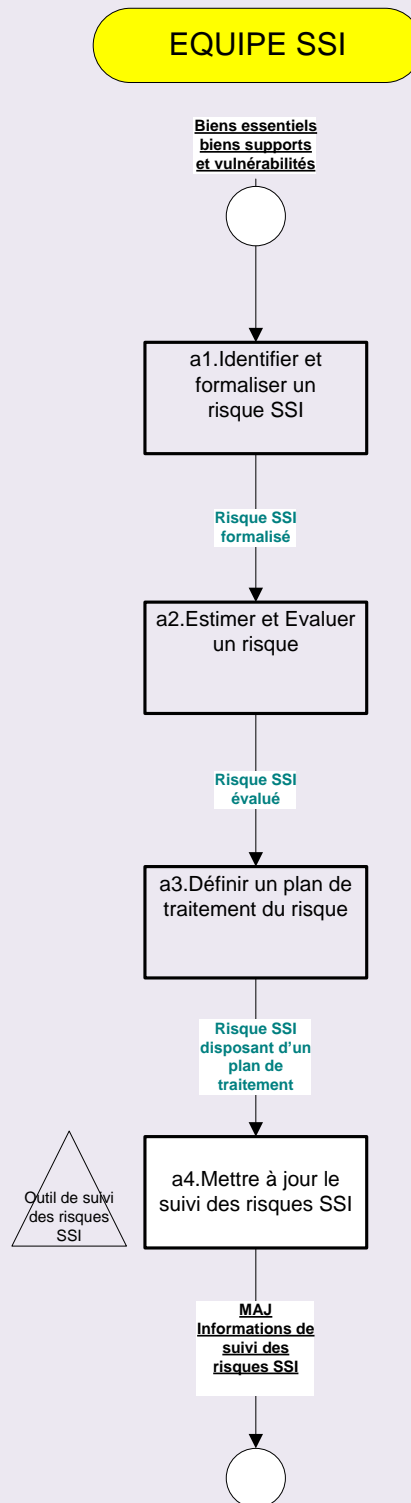


Figure 5 : activité A. Appréciation et proposition de traitement des risques

5.1.1 Etape a1 : Identification des scénarios de risques

Acteurs :

- RSSI rattaché à la MOA

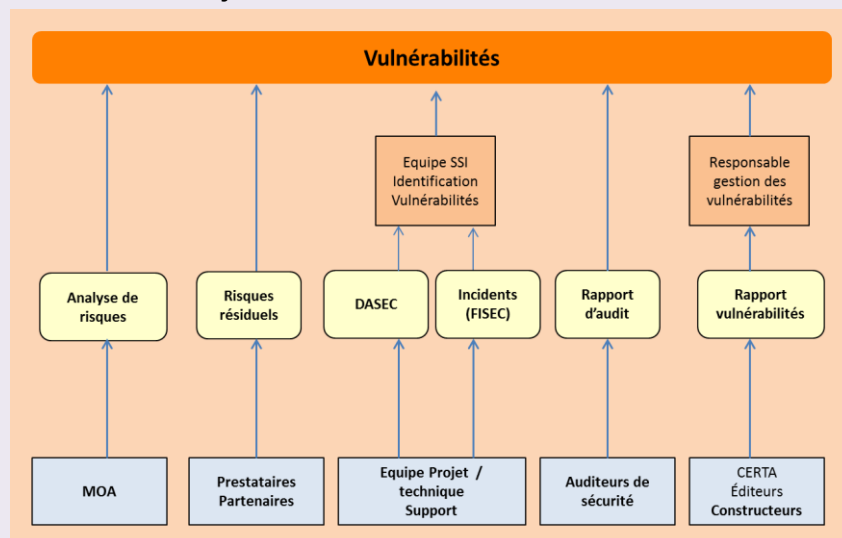
L'identification de risques numériques consiste à identifier les événements majeurs susceptibles de porter atteinte aux métiers ou à l'organisation du ministère de la justice, et à définir comment ces événements pourraient survenir et leurs conséquences potentielles.

Lors de cette première étape, le RSSI rattaché à la MOA identifie des scénarios risques, à partir des vulnérabilités numériques portées à sa connaissance, ainsi que sa connaissance des actifs primordiaux et des supports du système d'information visé.

5.1.1.1 Sources d'identification des vulnérabilités

Les principales sources d'identification de vulnérabilités numériques peuvent être :

- L'**analyse de risques**, si existante (synthèse des risques résiduels);
- Etude d'impact sur la vie privée (RGPD), le cas échéant ;
- les **documents de sécurité** des systèmes (PSSI/PES/DAT) ;
- les **résultats d'audit** (rapports d'audit) ;
- l'analyse des demandes d'avis sécurité (DASEC) ;
- les **fiches d'incidents de sécurité** (FISEC) ;
- les **données du CERT-FR** (et autres CERT, organismes similaires, éditeurs, constructeurs) ;
- les correspondants sécurité chez les partenaires du ministère de la justice.



5.1.1.2 Description du risque

Un scénario de risque est caractérisé par ses différentes composantes :

- **la source de menace**, qu'elle soit naturelle ou humaine, accidentelle ou volontaire, interne ou externe au ministère de la justice ;
- **la menace** ;
- **les vulnérabilités** susceptibles d'être exploitées ;
- **l'(es) actif(s) primordial (aux)** exposés aux impacts ;
- **l'(es) actif(s) en support(s)** concernés par les vulnérabilités ;
- **les conséquences/les impacts** de la réalisation d'un scénario de risque sur le système et l'organisation, en termes de :
 - sur le fonctionnement des missions ;

- financier (perte financière directe ou indirecte) ;
- image pour le ministère de la justice (atteinte à sa réputation) ;
- juridique (non-conforme aux lois et règlements) ;
- sur la vie privée (RGPD).

L'identification des composantes d'un risque doit tenir compte des mesures de sécurité existantes et de leur efficacité.

Par exemple, une mesure de sécurité incorrectement mise en œuvre, présentant un dysfonctionnement, ou encore utilisée de manière incorrecte peut constituer une vulnérabilité.

Lorsqu'un risque est identifié il doit être référencé suivant la convention définie à l'annexe 8.2.

5.1.2 Etape a2 : Estimation & évaluation des risques

Acteurs :

- Equipe SSI ou RSSI ;
- Acteurs opérationnels (en fonction du besoin) ;
- Maitrise d'ouvrage (principale ou déléguée, en fonction du besoin).

L'estimation des risques est basée sur l'appréciation de :

- **la vraisemblance du scénario** (la probabilité d'occurrence) ;
- **ses conséquences potentielles** (l'impact, la gravité).

La consolidation de ces éléments permet d'évaluer la **criticité** du risque.

Les mesures de sécurité existantes et leur efficacité peuvent permettre de réduire la vraisemblance d'une menace, la facilité à exploiter une vulnérabilité, ou encore limiter l'ampleur d'un incident.

L'estimation des risques peut être effectuée avec plus ou moins de précision.

Une estimation précise, passera généralement par la réalisation d'un audit qui permettra de déterminer plus précisément les vulnérabilités existantes et leur facilité d'exploitation. Pour garantir un niveau de cohérence globale dans l'estimation et l'évaluation des risques, il est fortement conseillé d'utiliser lors de l'audit des échelles identiques à celles employées dans le projet. Tous les ans, il est possible de sélectionner certains risques parmi ceux qui n'ont pas été couverts/traités, et les réévaluer si une étude plus poussée semble nécessaire.

5.1.2.1 Estimation de la vraisemblance du scénario

La probabilité d'occurrence d'un risque est fonction de la fréquence de survenance de la menace et de la facilité d'exploitation des vulnérabilités. Elle est évaluée sur une échelle allant de 1 à 4 :

1. **Faiblement probable** ou nécessite des moyens très importants et/ou des connaissances très élevées dans le domaine considéré ;
2. **Moyennement probable** (Modéré) ou nécessite un certain niveau d'expertise et/ou du matériel spécifique ;
3. **Probable** ou réalisable avec des moyens standards et/ou avec des connaissances de base ;
4. **Très probable** (Presque certain) ou réalisable par tout public.

Dans cette étape, le RSSI de la maitrise d'ouvrage (principale ou déléguée) peut s'appuyer sur l'expérience des équipes opérationnelles pour déterminer la probabilité d'occurrence d'un risque. L'historique des incidents de sécurité déjà survenus, ou les statistiques des risques survenus dans les organismes similaires, peuvent également aider à évaluer la probabilité d'occurrence.

5.1.2.2 Estimation des conséquences potentielles

L'impact sur les métiers ou l'organisation du ministère de la justice en cas de réalisation du risque est estimé en fonction de l'échelle suivante. Il est évalué sur une échelle allant de 1 à 4 :

1. **Faible ;**

2. **Modéré ;**
3. **Significatif ;**
4. **Grave.**

Dans cette étape, l'équipe SSI doit se rapprocher des équipes métiers responsables de « l'actif primordial » concerné par le scénario de risque, afin d'évaluer l'impact.

5.1.2.3 Estimation de la criticité

La criticité du risque est obtenue en croisant la probabilité d'occurrence et l'impact sur les métiers et/ou l'organisme.

$$\text{CRITICITE} = \text{PROBABILITE} \times \text{IMPACT}$$

La criticité permet de définir une priorité dans le traitement des différents risques. Elle est représentée dans la matrice ci-dessous.

| Probabilité d'occurrence Impact sur l'organisme | 1 - Faiblement probable / Moyens et/ou connaissances très importants | 2 - Moyennement probable / Moyens et/ou connaissances spécifiques | 3 - Probable / Moyens et/ou connaissances de base | 4 - Très probable / Réalisable par tout public |
|--|--|---|---|--|
| 4 - Grave | 4 | 8 | 12 | 16 |
| 3 - Significatif | 3 | 6 | 9 | 12 |
| 2 - Modéré | 2 | 4 | 6 | 8 |
| 1 - Faible | 1 | 2 | 3 | 4 |

Figure 6 : Echelle de criticité de risque

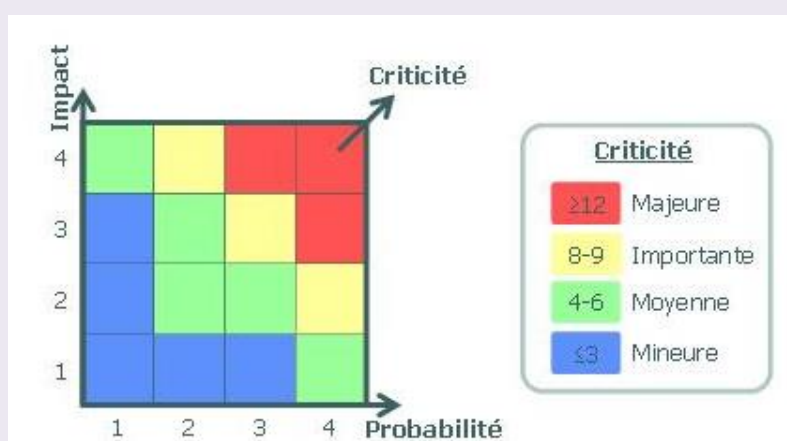


Figure 7 : Schéma de criticité des risques

L'AQSSI doit être alertée lors de l'identification d'un risque majeur qui doit être traité en priorité.

5.1.2.4 Evaluation des risques

L'évaluation des risques, consiste à sélectionner les risques qui sont retenus pour le traitement (les risques les plus critiques), et à prioriser cette liste de risques.

5.1.3 Etape a3 : Définition du traitement

Acteurs :

- Equipe SSI ou RSSI ;
- Equipes opérationnelles responsables du traitement des risques.

Lors de cette étape, une ou plusieurs solutions de traitement sont proposées pour les risques récemment identifiés.

Il existe 4 types de traitement possibles pour un risque :

- la **réduction du risque** qui consiste à définir les mesures organisationnelles et techniques susceptibles de couvrir le risque et de rendre le risque résiduel acceptable pour la MOA ;
- le **refus ou l'évitement du risque** qui consiste à abandonner les activités engendrant le risque, ou à modifier les conditions dans lesquelles elles doivent être réalisées afin de faire disparaître le risque du périmètre de la gestion des risques. Cette décision est prise lorsque le risque est trop important ou que le coût des opérations de traitement est trop élevé. Par exemple en cas de risque lié aux catastrophes naturelles, il peut être plus rationnel de déplacer le site de l'activité là où le risque n'existe pas ou là où il est sous contrôle ;
- le **transfert du risque** qui consiste à transférer la couverture d'un risque vers un tiers (seule la couverture du risque est transférée). Il peut s'agir par exemple de sous-traiter l'activité engendrant le risque afin que le partenaire assure lui-même la surveillance nécessaire du système d'information et entreprennent les actions nécessaires. Il peut aussi être fait appel à une assurance ;
- le **maintien du risque (acceptation)**, qui consiste à ne pas mettre en œuvre de plan d'actions pour traiter le risque, tout en assurant une surveillance constante de son évolution.

L'équipe SSI doit identifier les équipes opérationnelles concernées par le traitement du risque. Le plan de traitement sera ensuite défini conjointement entre l'équipe SSI et les équipes opérationnelles. Cependant, le choix du traitement des risques majeurs sera arbitré par la MOA (en comité de gestion des risques : étape b2 du point 5.2.2) et pourra l'être par l'équipe SSI dans tous les autres cas.

Dans le cas où il est décidé de « réduire » le risque, un plan d'actions est défini : composé d'une ou plusieurs « actions SSI » attribuées à des responsables d'actions (identifiés par l'équipe SSI). La complexité de mise en œuvre (coûts, charge ETP, disponibilité et compétences des ressources) du plan d'actions (une échelle est présentée à titre indicatif en annexe 8.3), et le niveau de criticité du risque résiduel après sa réalisation doivent être évalués. Pour chaque action, la date prévisionnelle de fin doit être communiquée par le responsable de l'action.

Pour « aiguiller » le traitement d'un risque, il est possible de s'appuyer sur la matrice présente en annexe 8.4 qui prend en compte la complexité du plan d'action ainsi que la criticité du risque.

Il peut être nécessaire de proposer plusieurs plans d'actions dans le traitement d'un risque, notamment lorsqu'il s'agit d'un risque majeur, et que le plan de traitement est complexe.

Dans le cas où un plan d'actions est transversal et/ou complexe, un « **chef de projet dédié** » pourra être nommé (étape b4 du point 5.2.4). Il sera responsable de coordonner les différentes entités intervenantes dans le plan d'action et pourra obtenir pour cela une délégation de pouvoir. La désignation du chef de projet pourra être arbitrée en « comité de gestion des risques ».

5.1.4 Etape a4 : Mise à jour du suivi des risques

Acteurs :

- Equipe SSI ou RSSI.

Lors de cette étape, l'ensemble des informations relatives aux nouveaux risques identifiés et aux plans de traitement proposés, sont reportés dans le suivi centralisé des risques SSI, par l'équipe SSI (outil de suivi).

5.2 Activité B Suivi du traitement des risques SSI

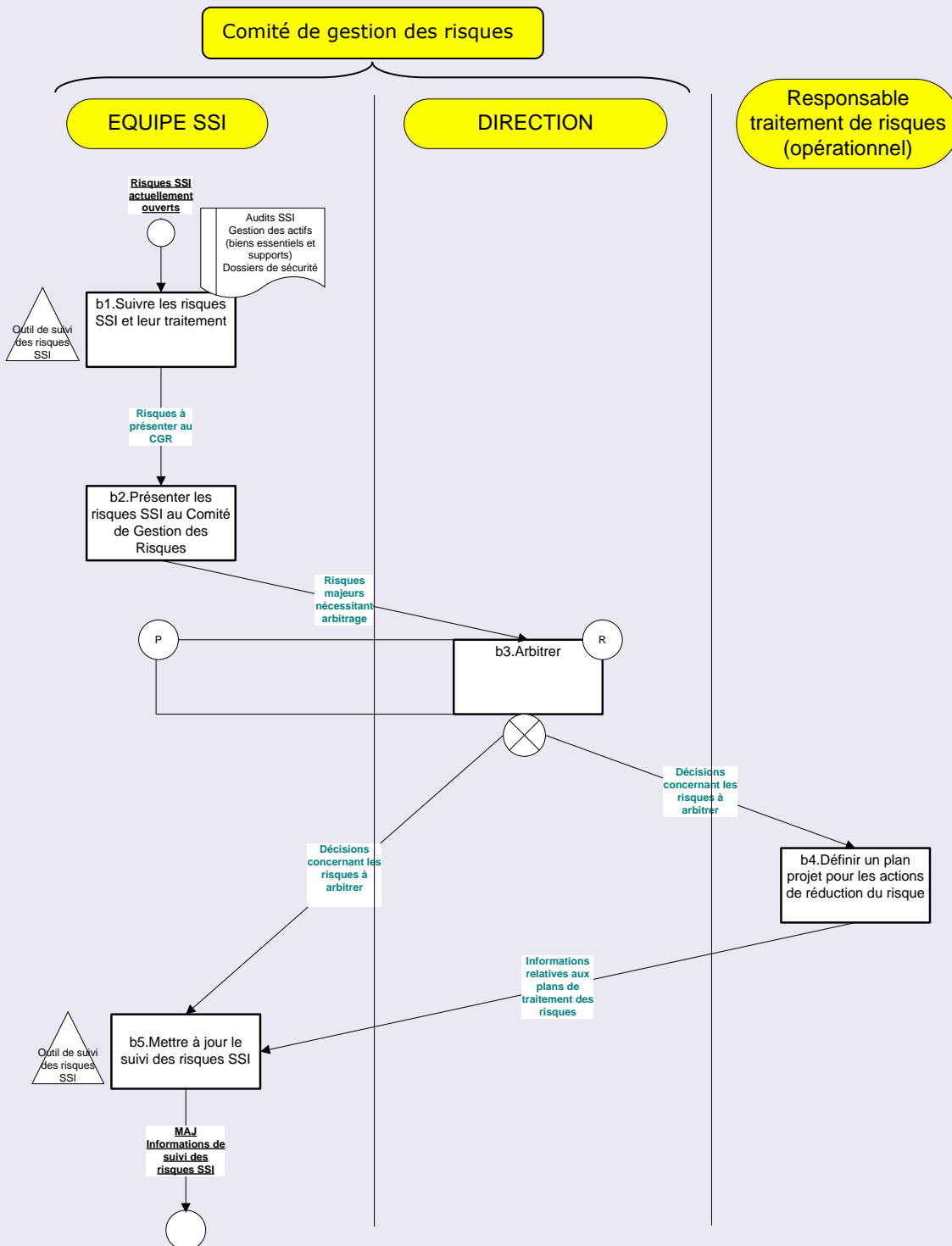


Figure 2 : activité B. Appréciation et proposition de traitement des risques

5.2.1 Etape b1 : Suivi des risques et de leur traitement

Acteurs :

- Directeur ou chef de projet MOA ;
- Equipe SSI ou RSSI ;
- Equipes Opérationnelles.

Lors de cette étape, l'équipe SSI effectue le suivi d'avancement des « actions SSI » pour l'ensemble des risques en cours de traitement.

Le but est :

- de contrôler l'avancement de chaque plan de traitement des risques ;
- d'identifier les plans de traitement clôturés (plan d'actions totalement mis en œuvre) ;
- d'identifier les plans d'actions qui ont des difficultés à aboutir (plans de traitement « bloqués »).

Ce suivi s'effectue auprès des responsables d'actions ou chefs de projet (équipes opérationnelles) identifiés à l'étape a3 du point 5.1.3. Les informations collectées sont reportées dans le suivi centralisé des risques numériques par l'équipe SSI.

Lorsque la mise en œuvre du plan d'action présente des difficultés, celles-ci doivent être remontées à l'équipe SSI, et, le cas échéant, seront débattues, pour arbitrage, au Comité de gestion des risques (étape b3 du point 5.2.3).

5.2.2 Etape b2 : Présentation au Comité de gestion des risques

Acteurs composant le comité de gestion des risques :

- Directeur ou chef de projet ;
- AQSSI ou son représentant ;
- RSSI ;
- Représentants de la MOA, responsables de l'arbitrage des risques.

Le suivi de l'ensemble des risques SSI doit être présenté régulièrement au comité de gestion des risques.

L'objectif sera de mettre en exergue les nouveaux risques majeurs, ainsi que l'avancement des plans de traitement relatifs aux risques majeurs précédemment identifiés. La tenue de ce comité pourra également être l'occasion d'arbitrer les plans de traitement des risques majeurs complexes (étape b3 au point 5.2.3).

Une attention particulière sera portée pour faire ressortir les risques en état « bloqué » (c.à.d. dont le traitement n'avance pas), et nécessitant un arbitrage.

La restitution pourra prendre la forme :

- d'une synthèse de l'ensemble des risques SSI (en volumétrie), et des tendances d'évolution ;
- d'une cartographie des risques majeurs par sous-systèmes.

Des indicateurs concernant la gestion des risques par les tiers (ex : Tiers mainteneur, ...) pourront également être présentés.

5.2.3 Etape b3 : Arbitrage par le Comité de gestion des risques

Cette étape consiste à faire accepter ou non certains risques numériques par les représentants de la MOA, ou de leur faire choisir, parmi plusieurs, des plans de traitement proposés pour un risque, et à enregistrer formellement cette décision.

Cela se traduit soit par :

- la décision de **ne pas mettre en œuvre de plan d'action** permettant de couvrir un risque, ce qui revient à **accepter le risque en justifiant la décision** (ex : pérennité limitée du plan d'actions, coût de la solution trop élevée, ...) ;

- la décision de **mettre en œuvre le plan d'action partiellement ou dans sa totalité**, et à **accepter le risque résiduel** éventuel.

Dans l'hypothèse où le risque résiduel ne remplirait toujours pas les critères d'acceptation par la MOA, une nouvelle itération du traitement des risques peut s'avérer nécessaire avant de procéder à un nouvel arbitrage.

Chaque risque majeur et son (ses) plan(s) d'actions doivent être présentés au Comité de gestion des risques par l'équipe SSI.

Un compte rendu sera réalisé à l'issue de la tenue du comité afin d'enregistrer :

- l'acceptation des risques majeurs pour lesquels les plans d'actions ont été refusés ;
- l'acceptation des risques résiduels dans le cas où les plans d'actions ont été acceptés.

A la suite de ce comité, les décisions prises en matière de traitement des risques sont reportées par l'équipe SSI dans le suivi centralisé des risques SSI, et communiquées aux personnes concernées.

5.2.4 Etape b4 : Définition d'un plan projet

Acteurs :

- Directeur de projet ou Chef de projet de traitement d'un risque ;
- Equipe SSI.

Après validation du plan de traitement synthétique par le comité de gestion de risques, le chef de projet définit un plan projet détaillé. Ce plan projet est validé par le chef de service du SSIC ou son représentant et, en tant que de besoin, par le FSSI. Il fera l'objet d'un suivi régulier (comme pour les actions de traitement présentées à l'étape b1 du point 5.2.1).

5.2.5 Etape b5 : Mise à jour du suivi des risques

Acteurs :

- Equipe SSI.

Lors de cette étape, l'ensemble des informations relatives aux décisions prises en comité de gestion des risques (état d'avancement du traitement de risques et plan projet de traitement des risques) sont mises à jour, par l'équipe SSI, dans un document de suivi centralisé des risques numérique.

6 SURVEILLANCE ET REVUE DES RISQUES

Acteurs :

- Equipe SSI ou RSSI ;
- Responsables du traitement des risques (AQSSI).

6.1 Revue annuelle complète des risques

Une fois par an, l'ensemble des risques ouverts doit être passé en revue, afin notamment d'identifier les risques « bloqués » et de définir les actions à mener pour faire évoluer la situation.

Une synthèse des risques par entités du ministère de la justice est adressée annuellement au FSSI.

6.2 Surveillance et revue des facteurs de risques

Les risques sont surveillés et régulièrement revus, en particulier lors d'évolutions des activités de la MOA ou de modifications importantes du contexte d'emploi.

Les risques et les facteurs de risques (valeurs des biens, impacts, vulnérabilités, menaces, probabilité d'occurrence) sont passés en revue de manière régulière afin que tout changement puisse être identifié au plus tôt.

Ceci permet aussi de maintenir en permanence une vision opérationnelle des risques.

L'AQSSI doit ainsi s'assurer, en lien avec les RSSI, que l'ensemble des éléments suivants sont pilotés de manière continue :

- l'intégration de tout nouvel élément dans le périmètre de la gestion de risques ;
- les modifications de valeur des différents biens ;
- les nouvelles menaces qui pourraient apparaître ;
- la possibilité que de nouvelles vulnérabilités apparaissent ou que des vulnérabilités changent ou s'aggravent ;
- l'accroissement de la criticité de certains risques de telle manière qu'ils deviennent inacceptables ;
- la surveillance des moyens de protection, dont l'intégrité est une garantie de protection contre les risques.

Des changements majeurs dans l'organisation (changement de version applicative ou externalisation d'une activité par exemple) devront donner lieu à des revues plus approfondies des risques et de leur traitement.

6.3 Gestion des risques des services opérés par des « tiers »

Les « tiers » qui fournissent un service critique au ministère (ex : support, TMA, TMT, ...) doivent mener une analyse de risques initiale sur leur périmètre, la mettre à jour à intervalles réguliers et à chaque changement majeur.

Le suivi de ces risques (évaluation, avancement des plans d'actions de traitement, ...) doit être régulièrement (trimestriellement) transmis à l'équipe sécurité du service ou de la MOA concernée.

Les changements entraînant un risque de criticité importante ou majeure doivent être portés à la connaissance et autorisés par l'équipe sécurité du service ou de la MOA concernée.

Des audits devront être menés régulièrement sur le périmètre du tiers afin de s'assurer que les risques sont correctement identifiés et évalués, et que les plans d'actions pour réduire leur criticité sont menés suivant des délais acceptables.

Des accords devront être conclus avec le « tiers », afin qu'il s'engage à réduire les risques dans des délais acceptables, et des pénalités pourront être appliquées dans le cas où les engagements du tiers ne sont pas respectés.

Les risques identifiés par les tiers, doivent être évalués avec des échelles compatibles avec celles du ministère de la justice (dans l'idéal les échelles du ministère doivent être utilisées).

7 REVUE ET AMELIORATION DU PROCESSUS DE GESTION DES RISQUES

Dans le cadre de la mise en œuvre d'un SMSI, il est nécessaire de régulièrement surveiller, réexaminer et améliorer le processus de gestion des risques.

Des indicateurs seront mis en place, afin de piloter le processus de gestion des risques. Un certain nombre d'indicateurs sont présentés à l'annexe 8.5.

Le processus de gestion des risques fera l'objet d'une revue régulière (au minimum annuelle) dans le but d'une amélioration continue.

Périodiquement, les équipes sécurité s'assurent que les critères de mesures et d'évaluation des risques restent pertinents au regard des objectifs de l'organisation, de sa stratégie et sa politique et que les changements organisationnels et techniques sont bien pris en compte.

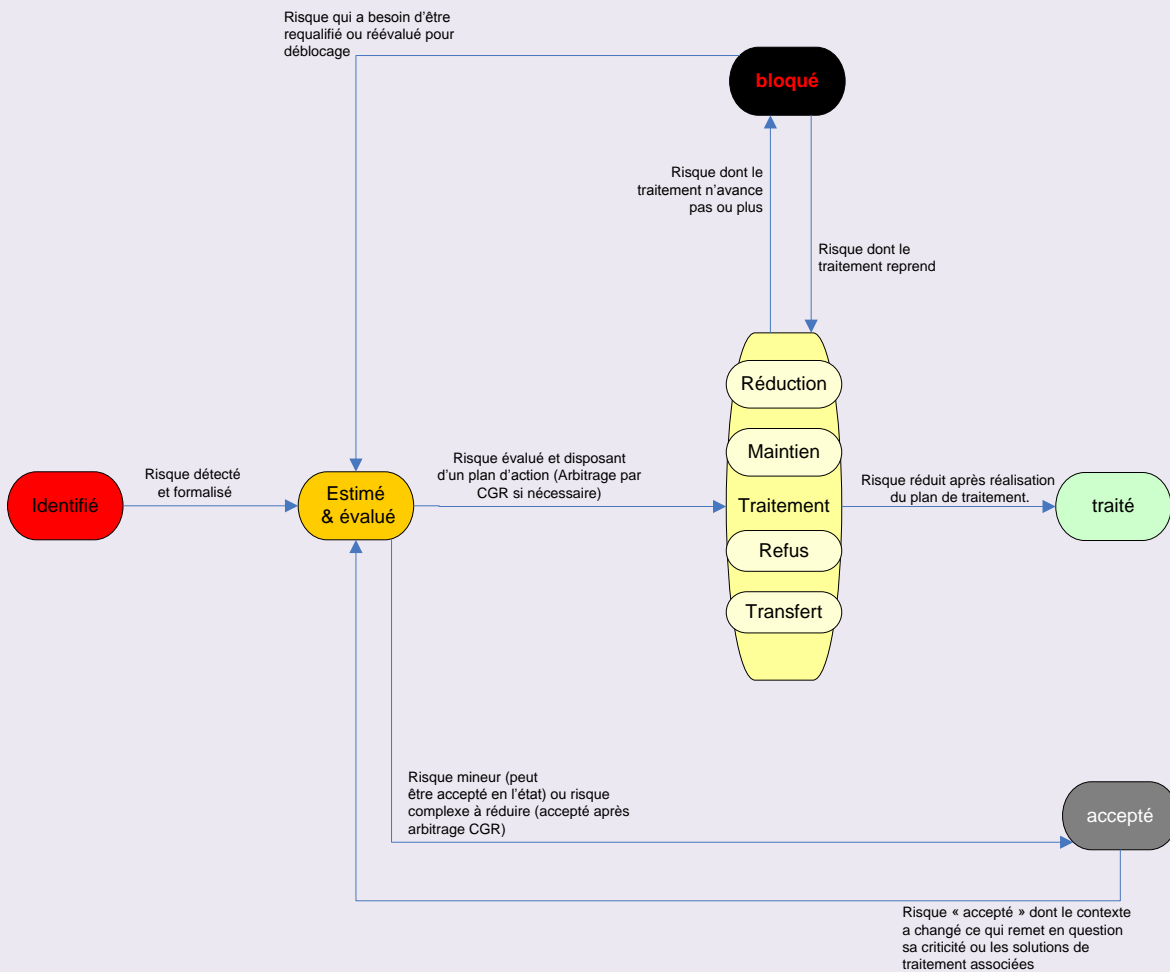
Il s'agit aussi de s'assurer que les plans d'actions et les plans de traitement restent pertinents au regard des circonstances.

Cette activité de pilotage et de revue devra concerner :

- l'approche d'analyse de risque ;
- les critères de mesures d'impacts ;
- les critères d'évaluation des risques ;
- les critères d'acceptation des risques ;
- les ressources nécessaires.

8 ANNEXES

8.1 Différents états d'un risque



Description des différents états :

- **identifié** : Le risque a été détecté / envisagé par une personne, dans le cadre d'une étude, d'un incident, d'un audit, d'une analyse, ... et décrit de façon formelle (éléments : source de menace, menace, vulnérabilité, biens impactés, scénarios d'incident,...) ;
- **estimé & évalué** : La criticité du risque a été calculée grâce à l'évaluation de la probabilité d'occurrence du scénario et l'impact en cas de réalisation. De plus, le risque a été priorisé par rapport aux risques détectés ;
- **en cours traitement** : Le plan d'actions visant à réduire le niveau du risque est en cours de réalisation ;
- **accepté** : Il a été admis qu'aucun plan d'actions ne sera réalisé pour réduire le niveau du risque, son niveau est donc « accepté » tel quel ;
- **bloqué** : Le plan d'actions visant à réduire le niveau du risque n'a pas débuté ou est stoppé pour des raisons diverses (ressources insuffisantes, disponibilité des équipes, responsabilités mal définies,...) ;
- **traité** : le plan d'actions visant à réduire le niveau du risque a été complètement réalisé.

8.2 Convention pour les références de risques

| | |
|-------------------|--|
| YY_R.SSI.DASEC_0X | Risque venant d'une Demande d'avis sécurité |
| YY_R.SSI.FISEC_0X | Risque venant d'une fiche d'incident sécurité |
| YY_R.SSI.AUDIT_0X | Risque venant d'un rapport d'audit |
| YY_R.SSI.DSEC_0X | Risque venant spécifiquement d'un dossier sécurité |
| YY_R.SSI.CERT_0X | Risque venant du CERTA ou d'un autre CERT |
| YY_R.SSI.TIERS_0X | Risque venant d'un tiers (prestataire ou partenaire) |
| YY_R.SSI.AUTR_0X | Risque venant d'une source non référencée précédemment |

Les références suivantes sont à utiliser lors de l'identification et l'enregistrement d'un nouveau risque.

YY : Correspondant à l'année où le risque est identifié.

0X : correspond au numéro du risque, +1 à chaque nouveau risque quelque soit sa source.

8.3 Métriques

- Besoins de sécurité

Echelle de confidentialité

| Niveau | Besoin | Définition |
|--------|---------------|---|
| 0 | Faible ou nul | L'élément essentiel peut être rendu public. |
| 1 | Restreint | L'accès à l'élément essentiel est restreint aux personnels ou processus internes autorisés de par leur fonction ou de par leur appartenance à une entité organisationnelle. |
| 2 | Confidentiel | L'accès à l'élément essentiel est restreint aux personnels ou process internes autorisés de par leur fonction ou de par leur appartenance à une entité organisationnelle, et qui par ailleurs ont le besoin d'en connaître. |
| 3 | Secret | Accès strictement restreint aux seuls personnels nommément désignés par la loi ou un règlement. |

Echelle de disponibilité

| Niveau | Besoin | Définition |
|--------|-----------------------------------|---|
| 0 | Faible | L'élément essentiel peut être indisponible pour une longue période |
| 1 | Disponibilité sous quelques jours | L'élément essentiel doit être disponible sous quelques jours |
| 2 | Disponibilité dans la journée | L'élément essentiel doit être disponible dans la journée, aux personnes qui ont le besoin d'en disposer |
| 3 | Disponibilité sans délai | L'élément essentiel doit être disponible sans délai aux personnes qui ont le besoin d'en disposer |

| Echelle d'intégrité | | |
|---------------------|----------------------|---|
| Niveau | Besoin | Définition |
| 0 | Faible | L'élément essentiel peut ne pas être intègre |
| 1 | Intégrité vérifiable | Besoin de détection du caractère intègre ou non intègre de l'élément essentiel sans correction nécessaire |
| 2 | Intégrité corrigible | Besoin de détection du caractère intègre ou non intègre de l'élément essentiel, avec correction requise si besoin |
| 3 | Intégrité totale | L'intégrité de l'élément essentiel doit être totale aussi bien pendant sa période d'utilisation qu'ultérieurement |

| Echelle de traçabilité | | |
|------------------------|------------------------------------|---|
| Niveau | Besoin | Définition |
| 0 | Faible ou nul | Aucun besoin de traçabilité |
| 1 | Besoin pour l'information | Besoin de traçabilité pour information, avec enregistrement éventuel d'une trace (non nécessairement détaillée) |
| 2 | Besoin de traçabilité systématique | Besoin de traçabilité pour information, avec enregistrement systématique d'une trace détaillée |
| 3 | Traçabilité légale | Besoin légal de traçabilité avec enregistrement systématique de trace comme élément de preuve indiscutable. |

- Gravité

| Echelle de gravité | | |
|--------------------|-------------|---|
| Niveau | Besoin | Définition |
| 0 | Négligeable | Le ministère surmontera les impacts sans aucune difficulté |
| 1 | Limitée | Le ministère surmontera les impacts malgré quelques difficultés |
| 2 | Importante | Le ministère surmontera les impacts avec de sérieuses difficultés |
| 3 | Critique | Le ministère ne surmontera pas les impacts. |

- Vraisemblance

| Echelle de Vraisemblance | | | |
|--------------------------|--------------------|--------------------|---------------------------|
| Niveau | Malveillance | Accident | |
| | Faisabilité | Connaissance du SI | Probabilité d' occurrence |
| Faible | Sans compétence | Aucune | Rare |
| Moyenne | Niveau élémentaire | Faible | Une fois par an |
| Forte | Solide compétence | Bonne | Une fois par mois |
| Maximale | Expert | Très bonne | Une fois par semaine |

8.4 Complexité de mise en œuvre

Il y a 4 niveaux de complexité possible pour un plan de traitement :

| |
|---------------|
| très complexe |
| Complexe |
| facile |
| très facile |

La complexité s'obtient en évaluant l'échéance et le budget nécessaire à sa réalisation :

| budget | échéance | | | |
|--------|---------------|---------------|---------------|---------------|
| | 1 | 2 | 3 | 4 |
| 4 | très complexe | très complexe | très complexe | très complexe |
| 3 | complexe | complexe | complexe | très complexe |
| 2 | facile | facile | complexe | complexe |
| 1 | très facile | très facile | facile | complexe |

a. échéance

| | 1 | 2 | 3 | 4 |
|----------|-----------------|------------|------------|----------------|
| Echéance | 1 mois ou moins | 1 - 3 mois | 3 - 6 mois | plus de 6 mois |

L'échéance prend en compte la disponibilité des personnes en interne, la charge jour/homme pour réaliser le plan d'action, le besoin de formation ou de trouver une ressource experte dans un domaine particulier.

b. budget

| | 1 | 2 | 3 | 4 |
|--------|----------------------|-----------------|------------------|-----------------------|
| budget | moins de 10000 euros | 10 000 - 50 000 | 50 000 - 100 000 | plus de 100 000 euros |

Intégrer dans le budget les couts de prestation et évaluer le coût de la charge interne à une valeur moyenne (ex : 1J/homme = XXX euros).

8.5 Aiguillage traitement des risques

| complexité | criticité | | | |
|---------------|-----------|---------------|--------------|--------------|
| | Mineur | Moyen | Important | Majeur |
| Très complexe | Suivi | Arbitrage | Arbitrage | Arbitrage |
| Complexe | Suivi | Arbitrage | Arbitrage | Arbitrage |
| Facile | Suivi | Traitement NP | Traitement P | traitement P |
| Très facile | Suivi | Traitement NP | Traitement P | traitement P |

- **Suivi** : Ces risques peuvent être acceptés avec un suivi régulier.
- **Traité de façon non prioritaire** : Ces risques n'ont pas une criticité élevée (moyen), ils seront tout de même réduits, car le plan d'action associé est simple.
- **Traité de façon prioritaire et présenté pour info au comité de gestion des risques** : Les risques sont important et majeurs, et la complexité des plans d'actions est faible (très facile, facile), les risques seront réduits de façon prioritaire et le plan d'actions sera présenté succinctement pour information au « Comité de gestion des risques ».
- **Présenté pour arbitrage (en comité de gestion des risques)** : ces risques ont :
 - o une criticité intermédiaire (moyen) et la complexité des plans d'actions proposés pour les réduire est importante (complexe, très complexe).
 - o Une criticité importante et majeure dont le plan d'actions a une complexité élevée (complexe, très complexe).

Ces risques doivent être présentés au « Comité de gestion des risques » pour arbitrage.

Le « Comité de gestion des risques » doit décider d'appliquer l'un des plans d'actions proposés (dans l'idéal, plusieurs plans d'actions doivent être proposés) ou d'accepter le risque. Les avantages/inconvénients/pérennité de chaque plan d'actions doivent être présentés afin d'aider à la décision.

8.6 Indicateurs du processus de gestion des risques

A des fins pragmatiques et dans la mesure où la gestion des risques se met en place, un seul indicateur (voir ci-dessous) sera pris en compte.

| Indicateurs | Méthode de calcul | Signification | Responsable |
|--------------------------|--|--|-------------|
| Taux d'efficacité | Nombre de risques traités/Nombre de risques totaux | Le nombre de risque traités est le nombre de risques acceptés ou effectivement traités (dont le plan d'action a été réalisé). Permet d'évaluer le niveau d'efficacité de la procédure de gestion des risques (exigence de l'ISO9001) | AQSSI |

D'autres indicateurs seront à considérer plus tard (augmentation de la maturité organisationnelle et de l'outillage)

| Indicateurs | Méthode de calcul | Signification | Responsable |
|--|---|--|-------------|
| Nombre de risques détectés | Recenser le nombre de risque détectés sur une année | Permet d'analyser l'efficacité des dispositifs de couverture des risques | |
| Nombre de risque par sous système | Après affectation des risques aux différents sous-systèmes, recenser le nombre de risque détectés par sous système | Permet d'analyser l'efficacité des dispositifs de couverture des risques par sous-systèmes. Permet d'identifier les sous-systèmes les plus vulnérables | |
| Taux de risques traités | Nombre de fiches de risques closes suite à la réalisation du plan d'action / Nombre de risques détectés sur une année | Permet d'analyser l'efficacité du dispositif de gestion des risques. | |
| Taux de risque en cours de traitement | Nombre de fiches de risques en cours de traitement / Nombre de risques détectés sur une année | Permet d'évaluer l'évolution du nombre de risque pouvant faire l'objet d'un traitement | |
| Taux de risques acceptés | Nombre de fiches de risques acceptées / Nombre de risques détectés sur une année | Permet d'évaluer l'évolution de l'exposition aux risques résiduels | |
| Délai moyen de clôture d'une fiche | Moyenne de la durée entre l'ouverture d'une fiche (détection du risque) et sa clôture | Permet de mesurer l'efficacité des phases de traitement et d'acceptation du risque | |
| Coût moyen des plans d'actions | Moyenne du coût des plans d'action | Permet de mesurer le coût moyen des plans d'actions | |

Annexe 4 : procédure d'exploitation de sécurité type

[Nom du projet]

Table des matières

| | | |
|-----------|---|-----------|
| 1. | ADMINISTRATION ET ORGANISATION DE LA SECURITE | 45 |
| 1.1. | INTRODUCTION | 45 |
| 1.2. | DOCUMENTS DE REFERENCE | 45 |
| 1.3. | DESCRIPTION DU SYSTEME | 45 |
| 1.4. | HISTORIQUE ET VUE D'ENSEMBLE | 45 |
| 1.5. | DESCRIPTION DU SYSTEME | 45 |
| 1.6. | MODE D'EXPLOITATION | 45 |
| 1.7. | ACCREDITATION | 45 |
| 1.8. | RESPONSABILITES | 45 |
| 1.9. | AUTORITE DE SECURITE | 45 |
| 1.10. | OSSI | 45 |
| 1.11. | ADMINISTRATEURS | 45 |
| 1.12. | UTILISATEURS | 45 |
| 1.13. | DIFFUSION DES SECOPs | 46 |
| 1.14. | GESTION DES UTILISATEURS ET DE LEURS DROITS | 46 |
| 1.15. | SIGNALEMENT DES INCIDENTS DE SECURITE | 46 |
| 1.16. | PROCEDURES DE CONTROLE APPLICABLES AUX SUPPORTS AMOVIBLES OU MATERIELS PRIVES | 46 |
| 1.17. | SECURITE DES TELECOMMUNICATIONS | 46 |
| 2. | SECURITE PHYSIQUE | 46 |
| 2.1. | IDENTIFICATION DES ZONES SENSIBLES | 46 |
| 2.2. | EMPLACEMENTS DES EQUIPEMENTS | 46 |
| 2.3. | GESTION DES CLES ET DES COMBINAISONS | 46 |
| 2.4. | CONTROLE D'ACCES | 46 |
| 2.5. | CONTROLE DES EQUIPEMENTS | 46 |
| 2.6. | GESTION DES ALARMES ET DE LA SECURITE | 46 |
| 2.7. | SECURITE PHYSIQUE EN DEHORS DES HEURES DE TRAVAIL | 46 |
| 3. | SECURITE DES PERSONNES | 46 |
| 3.1. | LISTE DU PERSONNEL | 46 |
| 3.2. | HABILITATIONS | 46 |
| 3.3. | FORMATION A LA SECURITE | 47 |
| 3.4. | LISTE DES ACCES AUTORISES | 47 |
| 3.5. | PERSONNEL DE MAINTENANCE ET D'ENTRETIEN | 47 |
| 4. | SECURITE DES DOCUMENTS | 47 |
| 4.1. | IDENTIFICATION DES DOCUMENTS | 47 |
| 4.2. | INSPECTIONS D'ENREGISTREMENTS ET RESPONSABILITES | 47 |
| 4.3. | CONTROLE, STOCKAGE ET MARQUAGE DES DOCUMENTS | 47 |
| 4.4. | CREATION, DIFFUSION ET RECEPTION DE DOCUMENTS | 47 |
| 4.5. | CONTROLE DES ENREGISTREMENTS | 47 |
| 4.6. | GESTION DES SUPPORTS INFORMATIQUES | 47 |
| 4.7. | DECLASSIFICATION ET DESTRUCTION | 47 |

| | | |
|-----------|--|------------|
| 5. | SECURITE DU SI | 47 |
| 5.1. | ENVIRONNEMENT SYSTEME | 47 |
| 5.2. | ENVIRONNEMENT MATERIEL | 47 |
| 5.3. | ARRET / DEMARRAGE DES MACHINES | 47 |
| 5.4. | CONNEXION ET DECONNEXION DE MATERIELS | 48 |
| 5.5. | CONTROLES D'INTEGRITE MATERIELLE | 48 |
| 5.6. | MAINTENANCE DU SYSTEME | 48 |
| 6. | SECURITE DU LOGICIEL | 478 |
| 6.1. | CONTROLE D'ACCES AU SYSTEME INFORMATIQUE | 48 |
| 6.2. | GESTION DES COMPTES UTILISATEURS | 48 |
| 6.3. | CONTROLE LORS DE L'INSTALLATION DE LOGICIELS | 48 |
| 6.4. | MASTERISATION LOGICIELLE ET COPIES DE SAUVEGARDE | 48 |
| 6.5. | GESTION DES TRACES D'AUDIT | 48 |
| 6.6. | ARCHIVAGE DES JOURNAUX D'AUDIT | 48 |
| 6.7. | PROTECTION CONTRE LES VIRUS | 48 |
| 6.8. | ZONAGE TEMPEST | 48 |
| 6.9. | GESTION DES EQUIPEMENTS CHIFFRE ET DES CLES ASSOCIEES | 48 |
| 6.10. | GESTION DES FILTRES DE SECURITE | 48 |
| 6.11. | MAINTENANCE DU LOGICIEL | 489 |
| 7. | PLAN DE SECOURS | 49 |
| 7.1. | SAUVEGARDE SYSTEMES ET SAUVEGARDE DES DONNEES UTILISATEURS | 49 |
| 7.2. | STOCKAGE ET ACCES AUX SUPPORTS DE SAUVEGARDE | 49 |
| 7.3. | REPRISE SUR INCIDENT MATERIEL | 49 |
| 7.4. | GESTION DES PERTES D'ALIMENTATION ELECTRIQUE | 49 |
| 7.5. | CLIMATISATION | 49 |
| 7.6. | GESTION DES PERTES DE MOYEN DE TELECOMMUNICATION | 49 |
| 7.7. | PROTECTION INCENDIE | 49 |
| 7.8. | MESURES D'URGENCE | 49 |
| 8. | GESTION DE CONFIGURATION | 49 |
| 8.1. | RESPONSABILITES POUR LA GESTION DE CONFIGURATION | 49 |
| 8.2. | CONFIGURATION DE REFERENCE | 49 |
| 8.3. | GESTION DES EVOLUTIONS MATERIELLES & LOGICIELLES | 49 |
| 9. | ANNEXES | 50 |
| A. | MISSIONS DE RESPONSABILITES DE L'OSSI | 50 |
| B. | MISIONS ET RESPONSABILITES DES ADMINISTRATEURS DU SI | 50 |
| C. | LISTE DES PERSONNELS | 50 |

1. ADMINISTRATION ET ORGANISATION DE LA SECURITE

1.1. Introduction

Cette partie décrit l'objectif ainsi que le champ d'application de la PES

1.2. Documents de référence

Cette partie consiste à identifier le référentiel documentaire de l'organisme (SI, SSI, aspects déontologiques et contractuels) qui servira de base à la suite de la démarche

- *Les aspects légaux et réglementaires (RGS, PSSIE, Loi 78-17 du 06/01/1978 modifiée...)*
- *Obligations contractuelles auxquelles l'organisme s'est engagé vis à vis de ses clients ou partenaires spécifiques*
- *Obligations contractuelles des prestataires ou partenaires*
- *Le référentiel de sécurité interne (schéma directeur informatique et SSI, analyses de risques, résultats d'audits...)*
- *Le référentiel du ou des systèmes d'information (directive d'exploitation, concept d'emploi...)*

1.3. Description du système

Ce paragraphe a pour objectif d'identifier globalement le système, son but, son fonctionnement et le situer dans son environnement pour déterminer précisément le périmètre d'action de la PES. Avant d'analyser les procédures de sécurité à mettre en œuvre, il est utile de définir précisément le système lui-même et d'en observer les frontières et ses limites.

Cette partie vise à fixer l'étendue de la PES et les entités sur lesquelles elle peut avoir une incidence. Les mesures écrites dans ce document doivent se limiter à un périmètre d'actions raisonnables (ni trop grand, ni trop petit).

1.4. Historique et vue d'ensemble

Pour la présentation concrète du SI, il faut avoir une vue générale du fonctionnement et chercher à découper le système en domaines fonctionnels (sous-ensemble) avec les interconnexions (flux de données) entre chaque domaine. Il est conseillé de faire une représentation graphique de l'architecture fonctionnelle du système. Le détail des domaines sera donné dans la partie suivante (description du système cible).

1.5. Mode d'exploitation

Le mode d'exploitation présente le contexte d'utilisation du système ainsi qu'une vue concrète de l'emploi du SI.

Le mode d'exploitation permet d'indiquer comment le système traite, transmet ou conserve des informations de sensibilités différentes pour des utilisateurs de catégories différentes. Il détermine à quel niveau les intervenants sur le système seront habilités et quel est leur besoin d'en connaître / modifier et d'en disposer.

1.6. Homologation

Ce paragraphe indique à quel niveau le SI est homologué ainsi que les éventuelles conditions d'emploi.

1.7. Responsabilités

1.7.1. Autorité de sécurité

Cette partie précise le rôle et les responsabilités de l'autorité de sécurité.

1.7.2. RSSI

Cette partie précise le rôle et les responsabilités de RSSI.

1.7.3. Administrateurs

Cette partie précise le rôle et les responsabilités de l'administrateur.

1.7.4. Utilisateurs

Cette partie précise le rôle et les responsabilités de l'utilisateur.

1.8. Diffusion des PES/SecOPs

Cette partie précise comment l'ensemble des PES génériques et locales sont rédigées, mises à jour et diffusées au personnel exploitant.

La mise en réseau de la PES, si son niveau de classification le permet, doit constituer un objectif, permettant aux utilisateurs d'accéder en permanence aux règles d'exploitation de sécurité.

1.9. Gestion des utilisateurs et de leurs droits

Ce paragraphe stipule la procédure de gestion des droits des utilisateurs (identifiant, accès système...)

1.10. Signalement des incidents de sécurité

Cette partie décrit le comportement d'exception permettant de traiter ces incidents de sécurité et les opérations à réaliser (acte réflexe, alerte, collecte d'information, expertise,...).

1.11. Procédures de contrôle applicables aux supports amovibles ou matériels privés

Cette partie précise les règles d'utilisation des supports et matériels personnels.

1.12. Sécurité des télécommunications

Cette partie décrit les mesures de sécurité liées aux télécommunications notamment en mentionnant les règles à respecter lors de l'usage de la messagerie électronique.

2. SECURITE PHYSIQUE

2.1. Identification des zones sensibles

Ce paragraphe définit les zones sensibles et les périmètres sensibles (espaces délimités par des « obstacles » pour l'accès au système, murs, portes, bureaux, ...).

2.2. Emplacements des équipements

Ce parape précise l'emplacement des équipements constituant le SI.

2.3. Gestion des clés et des combinaisons

Ce paragraphe décrit les procédures de gestions des clés et des combinaisons.

2.4. Contrôle d'accès

Ce paragraphe définit les contrôles physiques des accès à chaque périmètre (seul le personnel habilité doit avoir accès) et les modalités d'accès aux personnes non habilitées mais devant se rendre sur les lieux (lieu de livraison publique par exemple).

2.5. Contrôle des équipements

Ce paragraphe précise des mesures particulières de contrôle d'équipements (intégrité)

2.6. Gestion des alarmes et de la sécurité

Ce paragraphe décrit les procédures de gestion des alarmes et de la sécurité

2.7. Sécurité physique en dehors des heures de travail

Ce paragraphe précise les mesures de sécurité physique en dehors des heures de travail.

3. SECURITE DES PERSONNES

3.1. Liste du personnel

La liste des différents responsables intervenants sur système devra être renseignée en annexe C en précisant le niveau (administrateur, utilisateur...).

3.2. Habilitations

Ce paragraphe décrit les besoins d'habilitation des différents personnels (utilisateurs, administrateurs).

3.3. Formation à la sécurité

Ce paragraphe précise les formations nécessaires pour :

- *Le personnel impliqué dans la mise en œuvre du système : une formation adaptée à la réalisation de leurs tâches et fonctions sur le système.*
- *L'administrateur système / de sécurité : une formation spécifique sur la sécurité informatique et l'administration sécurisée d'un système d'exploitation.*

Il définit également le contenu et la fréquence des sensibilisations éventuelles.

3.4. Liste des accès autorisés

Ce paragraphe décrit les restrictions d'accès (documents, locaux).

3.5. Personnel de maintenance et d'entretien

Ce paragraphe décrit les procédures de gestion des personnels de maintenance et d'entretien.

4. SECURITE DES DOCUMENTS

4.1. Identification des documents

Ce paragraphe décrit les différents documents (technique ou non), en spécifiant les mesures de protection spécifiques.

4.2. Inspections d'enregistrements et responsabilités

Ce paragraphe précise les procédures d'inspections des enregistrements et les responsabilités.

4.3. Contrôle, stockage et marquage des documents

Ce paragraphe précise les mesures à mettre en œuvre pour le contrôle, le stockage et le marquage des documents.

4.4. Création, diffusion et réception de documents

Ce paragraphe indique les procédures de création, diffusion et réception de documents.

4.5. Contrôle des enregistrements

Ce paragraphe décrit les procédures de contrôle des enregistrements.

4.6. Gestion des supports informatiques

Ce paragraphe décrit les procédures de gestion des supports informatiques (de la mise en place au retrait).

4.7. Dé-classification et destruction

Ce paragraphe décrit les procédures de dé-classification et de destruction des documents (papier, support amovible)

5. SECURITE DU SI

5.1. Environnement système

Cette partie décrit l'environnement du système.

5.2. Environnement matériel

Cette partie décrit les mesures de protection contre la perte, l'endommagement, le vol, la compromission des biens du système (protection des documents classifiés, des supports amovibles, ...). On évoque l'emplacement, le stockage, la prise en compte, la manipulation ...

5.3. Arrêt / démarrage des machines

Cette partie précise la procédure d'arrêt et de démarrage des postes.

5.4. Connexion et déconnexion de matériels

Cette partie décrit les mesures de protection des services généraux. Protéger le matériel contre des coupures de courant et autres perturbations dues à une défaillance des services généraux (alimentation, énergie, climatisation).

Elle définit les matériels autorisés ainsi que les restrictions.

5.5. Contrôles d'intégrité matérielle

Ce paragraphe décrit les procédures de contrôle d'équipements (intégrité)

5.6. Maintenance des matériels

Cette partie définit les différents type de maintenance des matériels peut être de deux types : préventive ou curative et décrit les procédures dans les différents cas de réalisation de la maintenance : en interne ou en externe, par du personnel de l'organisme ou extérieur. Les périodicités et les méthodes à appliquer pour réaliser les opérations de maintenance préventive doivent être spécifiées par avance.

6. SECURITE DU LOGICIEL

6.1. Contrôle d'accès au système informatique

Ce paragraphe décrit les procédures de contrôle d'accès au SI.

6.2. Gestion des comptes utilisateurs

Ce paragraphe décrit les procédures de gestion des comptes utilisateurs.

6.3. Contrôle lors de l'installation de logiciels

Ce paragraphe décrit les procédures de contrôle de l'intégrité logiciel du système, de leurs paramètres de configuration par rapport à une version de référence.

6.4. « Masterisation » logicielle et copies de sauvegarde

Ce paragraphe décrit les procédures de « masterisation » et de sauvegarde logicielle.

6.5. Gestion des traces d'audit

Ce paragraphe décrit les procédures permettant de surveiller l'utilisation des moyens de traitement de l'information se déclinent selon :

- un contrôle des accès autorisés,*
- la gestion des alarmes de sécurité (antivirus) ou les défaillances (pannes),*
- un contrôle des modifications ou de tentatives de modification des paramètres ou mesures de sécurité.*

6.6. Archivage des journaux d'audit

Ce paragraphe précise les procédures de sauvegarde des fichiers permettant de retracer l'historique des faits (journaux).

6.7. Protection contre les virus

Ce paragraphe précise les procédures de mise en place les mesures de protection contre les codes malveillants (anti-virus, sas, machine blanche).

6.8. Zonage TEMPEST

Ce paragraphe précise les zones de protection à respecter : la zone de couplage et la zone de sécurité.

6.9. Gestion des équipements chiffre et des clés associées

Ce paragraphe décrit les procédures spécifiques de gestion des équipements chiffre et des clés associées.

6.10. Gestion des filtres de sécurité

Ce paragraphe spécifie la méthode de cloisonnement et précise les politiques de gestion.

6.11. Maintenance du logiciel

Cette partie définit les différents type de maintenance du ou des logiciels peut être de deux types : préventive ou curative et décrit les procédures dans les différents cas de réalisation de la maintenance : en interne ou en externe, par du personnel de l'organisme ou extérieur. Les périodicités et les méthodes à appliquer pour réaliser les opérations de maintenance préventive doivent être spécifiées par avance.

7. PLAN DE SECOURS

7.1. Sauvegarde systèmes et sauvegarde des données utilisateurs

Ce paragraphe décrit les responsabilités et la périodicité des sauvegardes systèmes et utilisateurs.

7.2. Stockage et accès aux supports de sauvegarde

Ce paragraphe décrit le stockage et accès des sauvegardes systèmes et utilisateurs

7.3. Reprise sur incident matériel

Ce paragraphe décrit les procédures de reprise après incident.

7.4. Gestion des pertes d'alimentation électrique

Ce paragraphe décrit les mesures de protection des matériels contre des coupures de courant et autres perturbations dues à une défaillance des services généraux (alimentation, énergie)

7.5. Climatisation

Ce paragraphe décrit les mesures de protection des matériels contre des perturbations dues à une défaillance de climatisation)

7.6. Gestion des pertes de moyen de télécommunication

Cette partie décrit les procédures de gestion des perte de moyen de télécommunication.

7.7. Protection incendie

Cette partie définit la protection incendie nécessaire à l'installation et utilisation du SI.

7.8. Mesures d'urgence

Ce paragraphe décrit les mesures d'urgence à appliquer.

8. GESTION DE CONFIGURATION

8.1. Responsabilités pour la gestion de configuration

Ce paragraphe précise les responsabilités du contrôle de l'intégrité matérielle et des logiciels du système, de leurs paramètres de configuration par rapport à une version de référence

8.2. Configuration de référence

Enumération détaillée des configurations matérielles et logicielles (noms des logiciels d'exploitation, des logiciels spécifiques, des progiciels et des utilitaires avec leurs numéros de version associés éventuellement au numéro de patch)

8.3. Gestion des évolutions matérielles & logicielles

Ce paragraphe décrit la procédure de gestions des évolutions matérielles et logicielles.

9. ANNEXES

A. Missions de responsabilités du RSSI

B. Missions et responsabilités des administrateurs du SI

C. Liste des personnels

Annexe 5 : décision d'homologation type

[Nom du projet]

SOMMAIRE

| | | |
|----|----------------------------------|----|
| 1. | INTRODUCTION | 44 |
| 2. | PRESENTATION DU SI | 44 |
| 3. | DECISION D'HOMOLOGATION FERME | 44 |
| 4. | AUTORISATION PROVISOIRE D'EMPLOI | 45 |

1. INTRODUCTION

1.1 Objet du document

Ce document vise à servir d'attestation formelle quant à la décision d'homologation prise par l'autorité d'homologation au regard de l'analyse du dossier d'homologation.

Ce document traduit la dernière étape de la démarche d'homologation d'un système.

1.2 Contexte

Ce paragraphe a pour objectif de rappeler le :

- Champs d'application du SI ;
- Cadre réglementaire applicable ;
- Référence à la note de mise en place de la commission d'homologation (= avis d'homologation).

2. PRESENTATION DU SI

Ce paragraphe reprend de façon synthétique les éléments structurants du dossier d'homologation, en précisant :

- Enjeux et missions du SI ;
- Besoins de sécurité ;
- Architecture du SI cible ;
- Interconnexions (si existant) ;
- Sites de déploiement.

3. DECISION D'HOMOLOGATION FERME

Le « Fonction de l'autorité d'homologation », représentant l'autorité d'homologation désignée par « référence et date du document »,

DECIDE

que le système d'information « Nom du SI » situé à « *Implantation géographique* » mis en place pour être utilisé dans le cadre de « cadre d'emploi » est homologué au niveau « Niveau retenu » dans la configuration présentée dans le dossier d'homologation [rappelée en annexe XXX].

La présente décision d'homologation est valable à compter du JJ/MM/AAAA jusqu'au JJ/MM/AAAA
Toute modification du système et / ou de son environnement annule la présente décision.

ATTACHE ET SIGNATURE

DESTINATAIRES :

COPIES :

4. AUTORISATION PROVISOIRE D'EMPLOI

Le **FONCTION DE L'AUTORITE D'HOMOLOGATION**, représentant l'autorité d'homologation désignée par **REFERENCE_ET_DATE_DU_DOCUMENT**

CONSIDERANT :

- soit un aspect opérationnel ;
- soit un risque accepté pour une durée limitée / un périmètre fonctionnel limité / un périmètre physique limité.

DECIDE

que le système d'information **NOM DU SI** situé à **IMPLANTATION GEOGRAPHIQUE** mis en place pour être utilisé dans le cadre de **CADRE D'EMPLOI** est homologué provisoirement au niveau **NIVEAU RETENU** dans la configuration présentée dans le dossier d'homologation [rappelée en annexe **XXX**] et sous réserve de condition suivante :

- soit de retrait du service à l'issue de l'APE ;
- soit de correction des faits constatés en vue d'une homologation complète et précisés en annexe **XXX** et dont les opérations seront conduites par **DESIGNATION DE L'AUTORITE**, directeur du système.

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

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

ATTACHE ET SIGNATURE

DESTINATAIRES :

COPIES :

Remarque : En fonction de la décision de l'autorité d'homologation le paragraphe 3 ou 4 s'applique.