MINISTÈRE
DES ARMÉES
*Liberté*
*Égalité*
*Fraternité*

# Mise et maintien en condition d'homologation

2022\CYBER\7\NP

# Table des matières

# 1 Introduction

Durant toutes les phases de la vie d'un projet, de nombreux éléments peuvent impact la démarche d'homologation initiale. La démarche présentée dans le présent document vise à maximiser dans les programmes de type « Cycle en V » ou « Agile » :

- La maîtrise des risques SSI
- La gestion de la dette SSI (ensemble des vulnérabilités résiduelles)

Elle conforte le processus d'homologation dans les deux phases de l'Instruction Ministérielle 1618 qui régit la conduite de programmes d'armement par la mise en œuvre des deux logigrammes présentés dans ce document de synthèse :

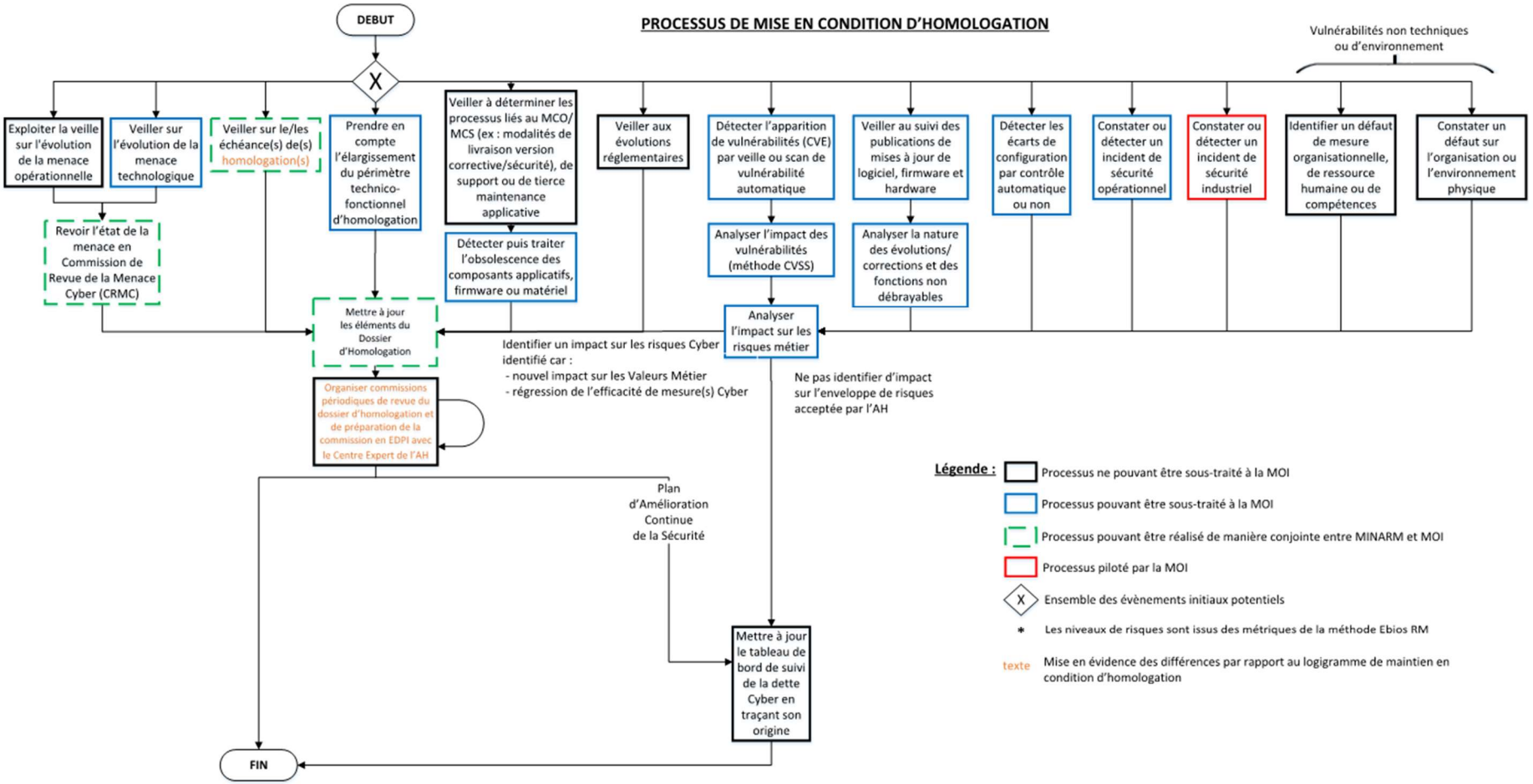
- Phase de « Réalisation » de l'IM1618 : mise en œuvre du logigramme « Mise en Condition d'Homologation » présenté ci-après
- Phase « d'Utilisation » de l'IM1618 : mise en œuvre du logigramme « Maintien en Condition d'Homologation » présenté ci-après

Ces réflexions ont été menées avec l'hypothèse d'une Autorité d'Homologation étatique (ex. Autorité d'Homologation Principale Inter-Armées, DGA, …), ils ont donc permis d'identifier, dans ces processus sous conduite étatique, l'ensemble des activités qui peuvent être déléguées à l'industrie. A noter que, dans le cas de systèmes sous Autorité d'Homologation industrielle, l'ensemble des activités décrites dans la synthèse peuvent être menées sous pilotage industriel.

# 2 Logigramme « Mise en Condition d'Homologation »

Le logigramme « Mise en Condition d'Homologation » a pour objectif de prendre en compte l'ensemble des événements alimentant le risques SSI et la dette SSI, ce, dès les premières phases d'un programme.

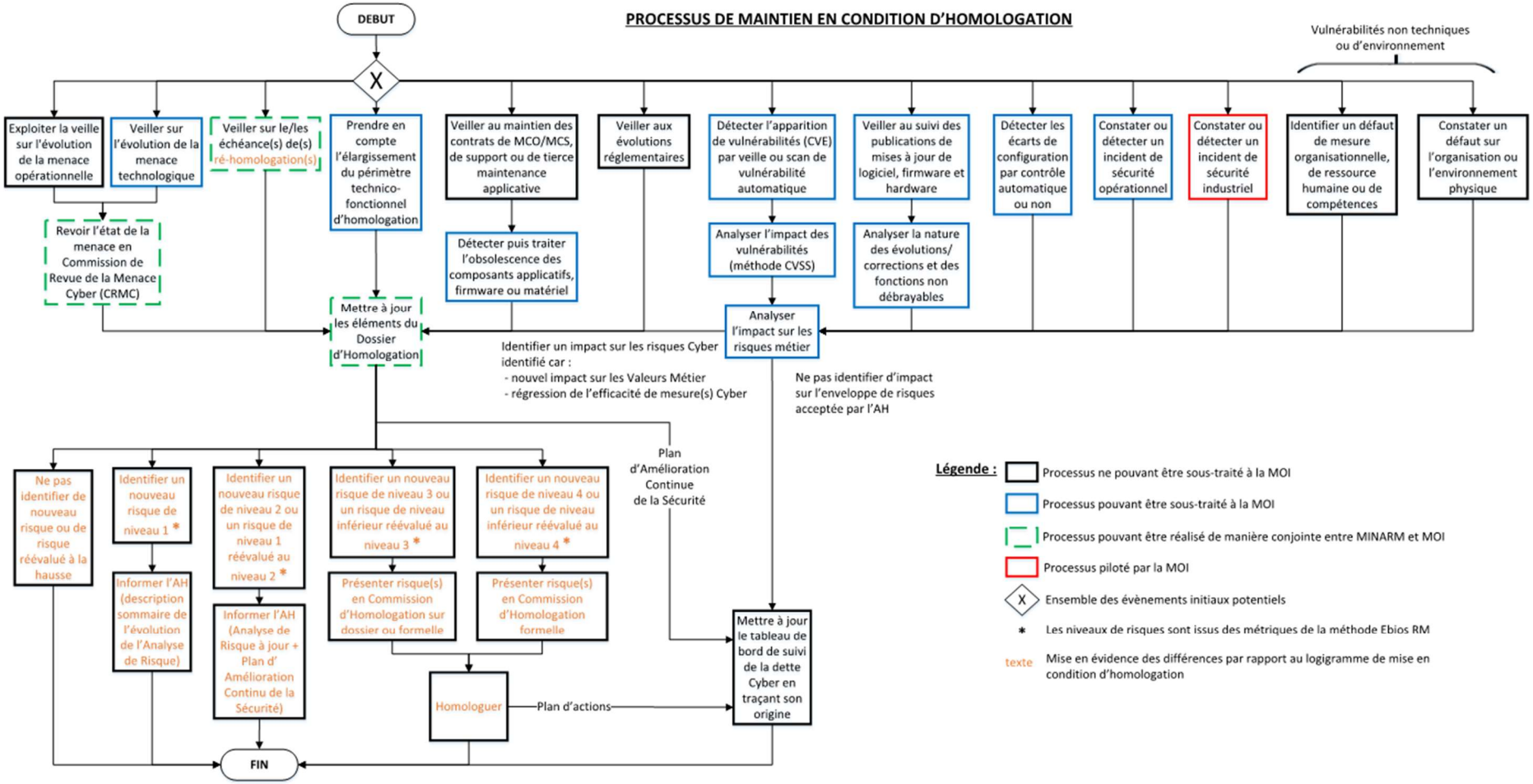
L'objectif étant de viser le déploiement d'un système « Cybersécurisé par conception » (« Secure By Design » en anglais), minimisant ainsi l'enveloppe de risques SSI résiduels, tout en assurant le suivi de la dette SSI identifiée lors du premier déploiement pour corrections ultérieures.



# 3 Logigramme « Maintien en Condition d'Homologation »

La grande finalité de l'homologation SSI est l'acceptation d'une enveloppe de risques jugée acceptable par l'AH.
Le logigramme ci-dessous a pour objectif de décrire le processus de « Maintien en Condition d'Homologation » ; chacun des sous-processus y étant décrit permettant de veiller à ce que l'enveloppe de risques préalablement acceptée par l'AH n'évolue pas à la hausse, tout en assurant un suivi de la dette SSI.

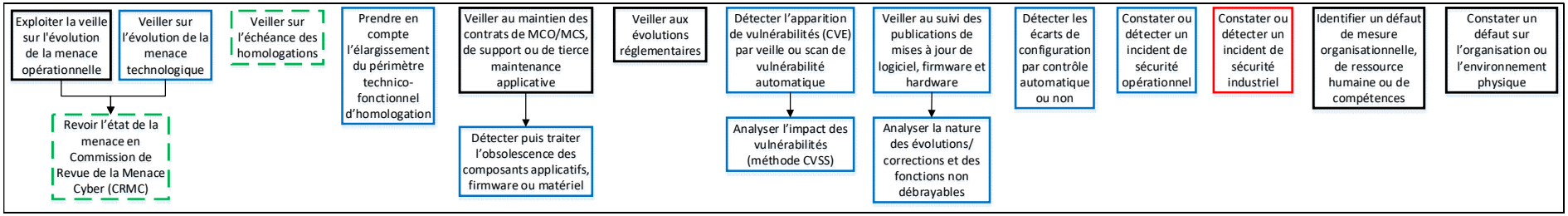
Il doit être mis en œuvre dès l'obtention de l'homologation et peut être annexé à la stratégie d'homologation quelle que soit son niveau (homologation capacitaire, homologation de services, …). Ceci permettant, dès la rédaction de la Stratégie d'Homologation (SH), de prendre des garanties sur la conduite de cette « veille » au Maintien en Condition d'Homologation dans le temps.




Les paragraphes suivants précisent l'usage du logigramme au travers de zooms sur ces différentes parties :

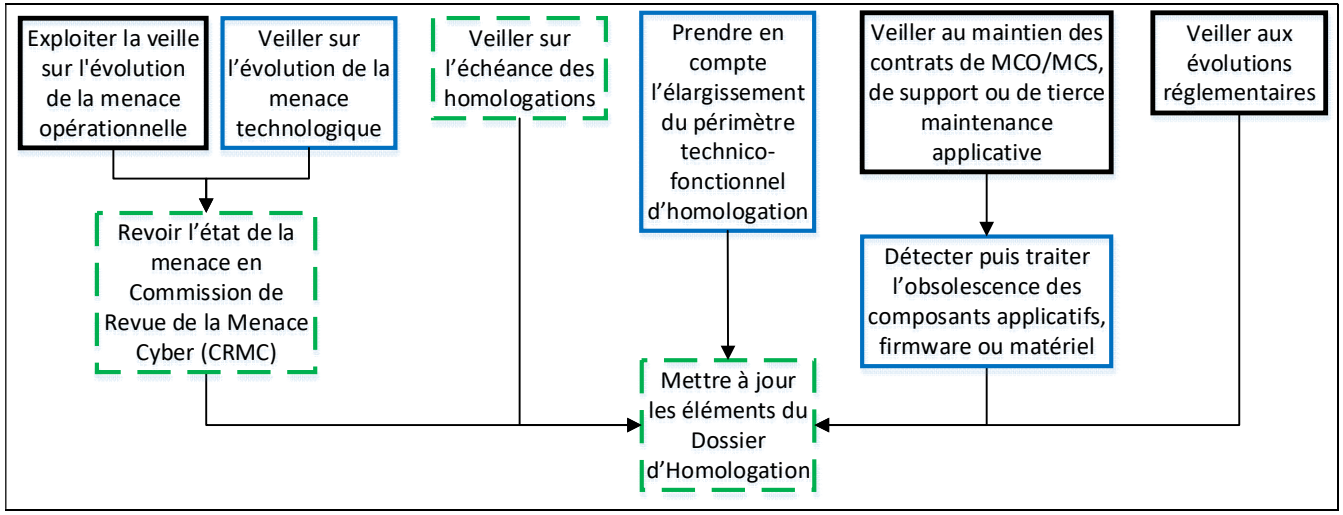
## *3.1 Zoom sur la seconde « ligne » du logigramme*

La seconde « ligne » du logigramme liste les processus permettant de détecter les événements pouvant avoir un impact sur les risques.




### 3.1.1 Les premiers processus de cette ligne

Les premiers processus nécessitent la mise à jour du dossier d'homologation : leurs sorties alimentent le processus « Mettre à jour le dossier d'Homologation ».

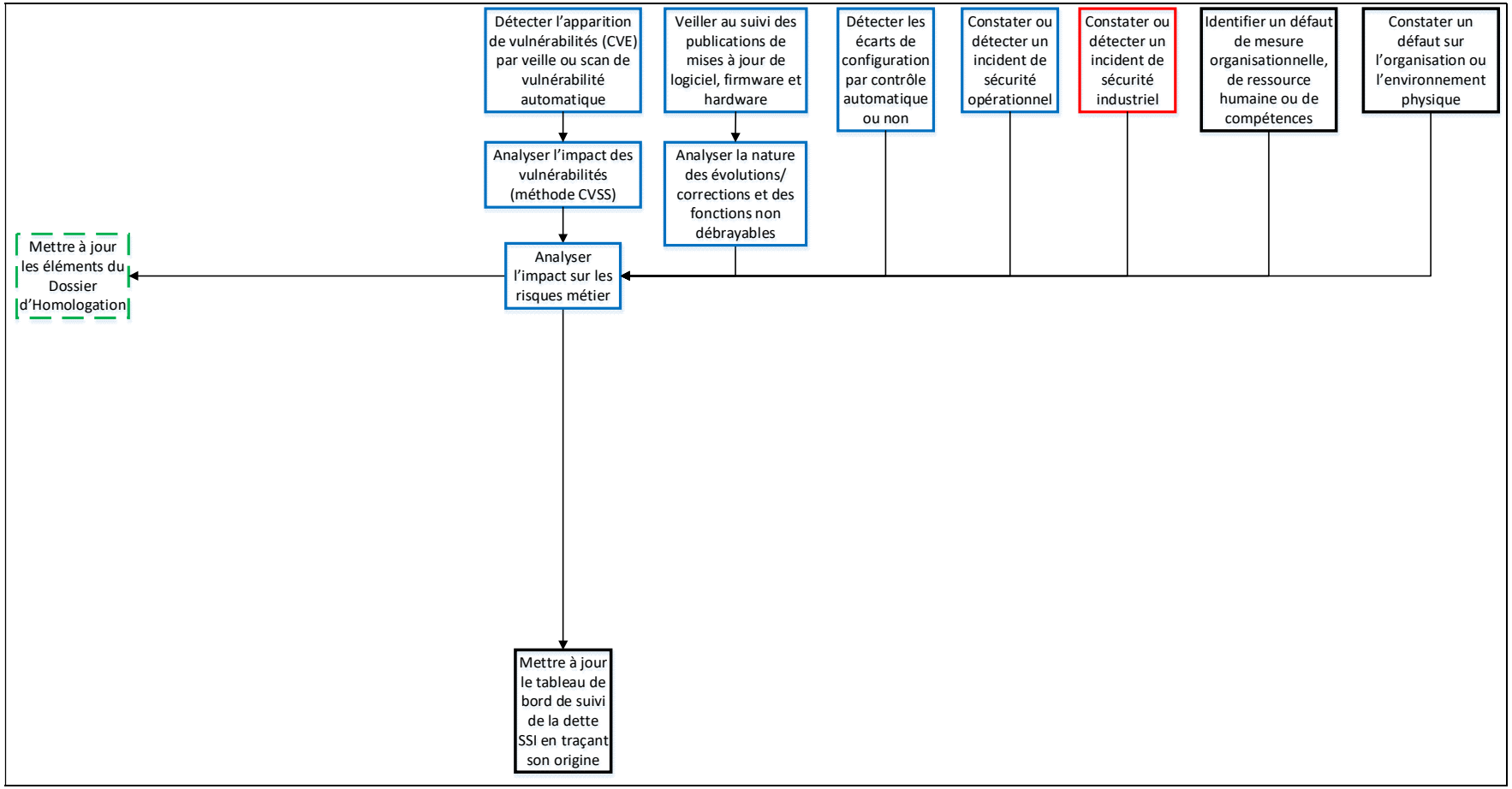



### 3.1.2 Les processus suivants

Les processus suivants nécessitent d'analyser leur(s) éventuel(s) impact(s) sur les risques (leurs sorties alimentent le processus « Analyser l'impact sur les risques métiers »).

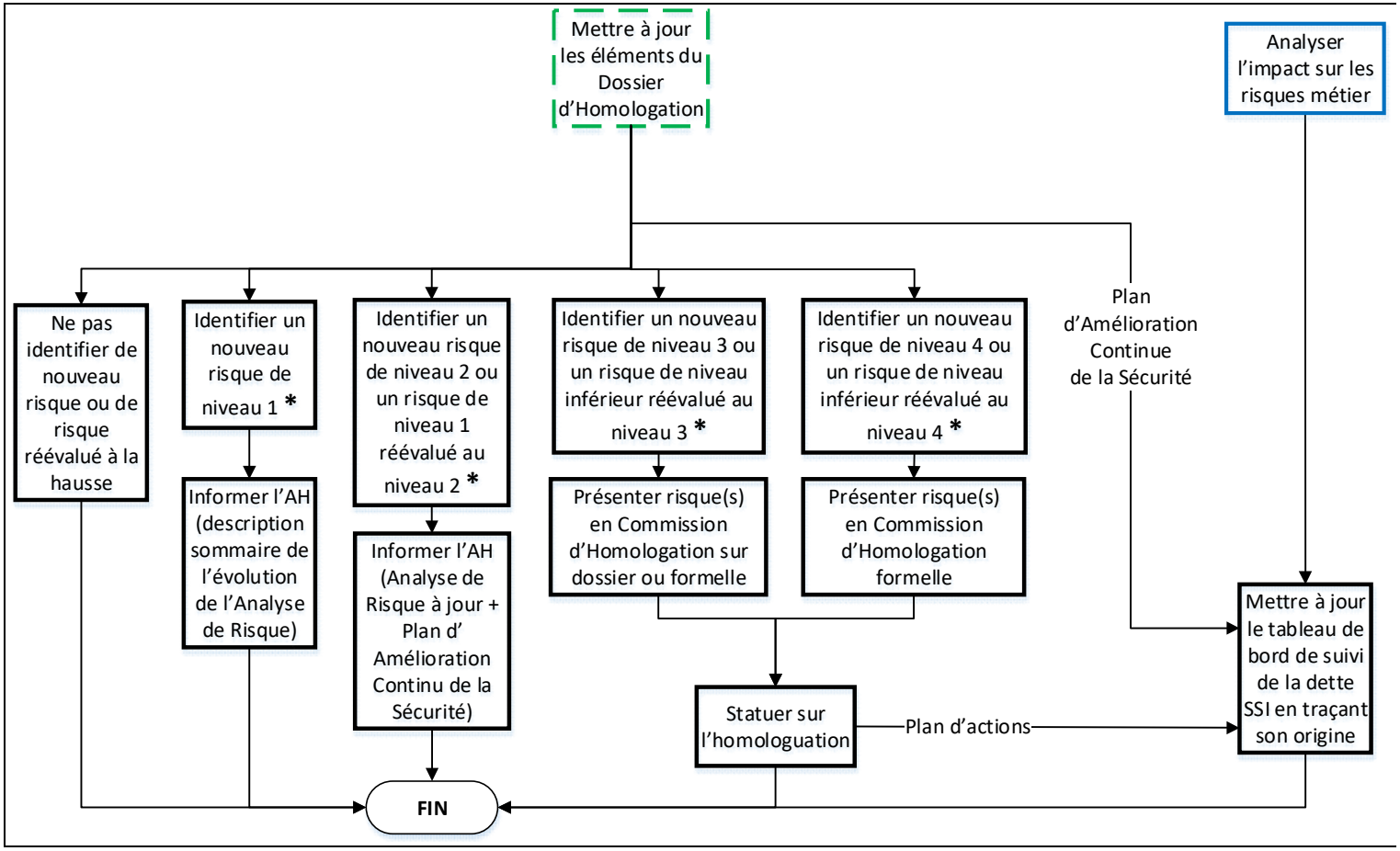
L'analyse d'impact sur les risques métiers peut avoir deux effets :

- d'une part, l'alimentation de la dette SSI,
- et d'autre part, l'alimentation du dossier d'homologation.




## *3.2 Zoom sur la partie basse du logigramme*

La partie basse du logigramme permet de traiter les éventuels impacts sur la décision d'homologation.
Les RH SSI étant contraintes, elle vise à mettre en œuvre un certain pragmatisme en décrivant la manière dont les saisines de l'AH sont effectuées au plus juste besoin, fonction de la métrique du niveau de risque définit dans la méthode EBIOS RM (le risque pouvant aller d'un niveau 1 (niveau le plus faible) à un niveau 4 (le niveau le plus élevé).


Mettre à jour les éléments du Dossier d'Homologation
Analyser l'impact sur les risques métier
Ne pas identifier de nouveau risque ou de risque réévalué à la hausse
Identifier un nouveau risque de niveau 1 *
Identifier un nouveau risque de niveau 2 ou un risque de niveau 1 réévalué au niveau 2 *
Identifier un nouveau risque de niveau 3 ou un risque de niveau inférieur réévalué au niveau 3 *
Identifier un nouveau risque de niveau 4 ou un risque de niveau inférieur réévalué au niveau 4 *
Plan d'Amélioration Continue de la Sécurité
Informer l'AH (description sommaire de l'évolution de l'Analyse de Risque)
Informer l'AH (Analyse de Risque à jour + Plan d' Amélioration Continu de la Sécurité)
Présenter risque(s) en Commission d'Homologation sur dossier ou formelle
Présenter risque(s) en Commission d'Homologation formelle
Statuer sur l'homologuation
Plan d'actions
Mettre à jour le tableau de bord de suivi de la dette SSI en traçant son origine
FIN

## 3.3 Détail des processus

| Numéro | Nom | Description | Données en entrée | Données en sortie | Pilote processus (Choix fait de ne pas faire de distinction faite entre RSSI-A et RSSI-P) | Contributeur(s) processus |
|---|---|---|---|---|---|---|
| 1 | Exploiter la veille sur l'évolution de la menace opérationnelle | Constater l'évolution de la composante opérationnelle de la menace pour l'ensemble du cycle de vie du système (maintenance, exploitation, etc...) ou de la capacité à laquelle il est rattaché | Bulletins d'information COMCYBER, GEMP, renseignement, Cyber Threat Intelligence industriels | État de la menace | RSSI | |
| 2 | Veiller sur l'évolution de la menace technologique | Constater l'évolution de la composante technique de la menace pour l'ensemble du cycle de vie du système (maintenance, exploitation, etc...).<br><br>À noter que ce sous-processus peut être délégué du MINARM aux MOI et éventuellement des MOI de rang 1 aux sous-traitants de rang 2. | Sources de veille | État de la menace | RSSI ou MOI | |
| 3 | Revoir l'état de la menace en Commission de Revue de la Menace Cyber (CRMC) | Commissions mixtes étatique/MOI plannifiées régulièrement avec ordre du jour fonction des sorties des sous-processus amont 1 et 2. | État de la menace issu des processus 1 et 2 | Document "Évolution de la menace" | RSSI ou MOI | |
| 4 | Veiller sur l'échéance des homologations | Rôle du RSSI de veiller à l'échéance des homologations.<br><br>Notifications (mail, appel) du chef de projet/RSSI possibles par le CHPI qui souhaite ménager son propre plan de charge et celui de l'AH.<br><br>Besoin d'anticipation sur les fins d'homologation pour s'accorder entre MINARM/MOI sur les impacts sur le dossier d'homologation et planifier en amont (prévoir également les éventuelles répercutions sur toute la chaîne des sous-traitants des MOI).<br><br>Le CHPI recommande qu'un plan d'amélioration continu de la SSI soit piloté par le RSSI-P avec réunions périodiques tous les 6 mois (préconisation CHPI) | Décision d'homologation précédente<br><br>CR et date du dernier audit (demandé tous les 3 ans) | Décision de lancer la mise à jour du dossier d'homologation et d'éventuelles actions associées (demande d'audit, saisine CHPI, ...)<br><br>Décision de mettre en oeuvre un plan d'amélioration continu de la sécurité reprenant notamment les actions issues de la décision d'homologation (ex : lancer demande d'audit, identifier les obsolescences,...).<br>=> rejoint le processus 30<br>(dde audit, saisine CHPI, ...) | RSSI ou MOI pour les plateformes chez l'industriel | CHPI / MOI / AF SSI |
| 5 | Prendre en compte l'élargissement du périmètre technico-fonctionnel d'homologation | Mettre à jour de l'analyse fonctionnelle, la vue matérielle issue de la conception, ... | Elargissement du périmètre | Dossier technico-fonctionnel à jour | RSSI | MOI / AF SSI |
| 6 | Veiller au maintien des contrats de MCO/MCS, de support ou de tierce maintenance applicative | Veiller au maintien des contrats ainsi qu'à leurs périmètres.<br><br>Prévoir un suivi des guides de durcissement ou des guides de recommandations de l'ANSSI | Date d'échéance des contrats<br>Source de la veille<br>Périmètre de la veille | Contrats mis à jour en terme de périmètre et renouvelés | RSSI | Equipe projet / MOI |
| 7 | Détecter puis traiter l'obsolescence des composants applicatifs, firmware ou matériel | Veiller auprès des éditeurs/fabriquants et fournisseurs à la fin de support SSI (MCS), fin de garantie ou fin de disponibilité commerciale. | Contrat / périmètre de veille | Proposition de plan de traitement des obsolescences (ex : proposer une solution de contournement, plan d'action de remplacement par un autre composant, ne rien faire et mettre en place des mesures organisationnelles,...). | RSSI ou MOI | |
| 8 | Veiller aux évolutions réglementaires | Organiser un GT SSI pour déterminer si cette nouvelle réglementation remet en cause ou pas son homologation | Nouvelles réglementation et documents associés (ex : nouvelle IGI 1300 avec nouvelle PSSI-M, nouvelle IM 900, Directive 27 ed3). | Dossier d'analyse et d'impact des évolutions réglementaires | RSSI | AF SSI / MOI / SSDI |
| 9 | Détecter l'apparition de vulnérabilités (CVE) par veille ou scan de vulnérabilité automatique | | Contrat : périmètre concerné, source(s) de la veille, ... | Rapports CVE concernant le système | RSSI ou MOI | |
| 10 | Analyser l'impact des vulnérabilités (méthode CVSS) | | Rapports CVE | Note CVSS (analyse d'impact contextualisée) avec plan de traitement préconisé (mesures techniques, mesures organisationnelles, mesures de contournement temporaires, ..., ainsi que l'ensemble de éléments de planification associés) | RSSI ou MOI | |
| 11 | Veiller au suivi des publications de mises à jour de logiciel, firmware et hardware | Evolutif et/ou correction de bugs | Périmètre concerné / source de veille (fournisseurs, ...) | Nouvelle version identifiée | RSSI ou MOI | |
| 12 | Analyser la nature des évolutions/corrections et des fonctions non débrayables | | Nouvelle version identifiée | Document d'analyse d'impact | RSSI ou MOI | |
| 13 | Détecter les écarts de configuration par contrôle automatique ou non | | Configuration initiale (de référence) | Écart par rapport à la configuration initiale | RSSI ou MOI | Equipe projet / Exploitant |
| 14 | Constater ou détecter un incident de sécurité opérationnel | - Constater (malware, audit, contrôle conformité, autre ...)<br>- Détecter (contrôle conformité automatique, cybersurveillance, autre...) | Description de l'incident | Constat / Rapport d'incident avec niveau de gravité | RSSI | Exploitant |

| | | | | | | |
|---|---|---|---|---|---|---|
| 15 | Constater au détecter un incident de sécurité industriel | - Constater (malware, audit, contrôle conformité, autre...)<br>- Détecter (contrôle conformité automatique, cybersurveillance, autre...) | Description de l'incident | Constat / Rapport d'incident avec niveau de gravité | MOI | |
| 16 | Identifier un défaut de mesure organisationnelle, de ressource humaine ou de compétence | | | Constat / Rapport | RSSI | |
| 17 | Constater un défaut sur l'organisation ou l'environnement physique | | | Constat / Rapport | RSSI | Exploitant |
| 18 | Mettre à jour les éléments du Dossier d'Homologation | Mettre à jour le dossier d'homologation :<br>- Analyse de risques + Plan d'Amélioration Continu de la Sécurité (PACS)<br>- Procédures d'Exploitation de la Sécurité (PES)<br><br>Sans oublier les nécessaires :<br>- Rapports de qualification et de tests de non-régression (métier et SSI)<br>- Configuration de référence et cartographie système<br>- Analyse d'impact sur les clients et l'environnement<br>- Stratégie de migration avec retour arrière si à | - Sortie des processus amont<br>- Autres :<br>-stratégie d'homologation<br>-??? | Dossier d'homologation à jour | RSSI | Centre Expert SSI / MOI / AF SSI |
| 19 | Analyser l'impact sur les risques métiers | | - Sortie des processus amont<br>- Autres :<br>-??? | | RSSI | Centre Expert SSI |
| 20 | Ne pas identifier de nouveau risque ou de risque réévalué à la hausse | | Analyse de risque à jour | | RSSI | Centre Expert SSI |
| 21 | Identifier un nouveau risque de niveau 1 | | Analyse de risque à jour | Nouveau risque identifié de niveau 1 | RSSI | Centre Expert SSI |
| 22 | Informer l'AH (description sommaire de l'évolution de l'AR) | | Analyse de risque à jour | | RSSI | Centre Expert SSI |
| 23 | Identifier un nouveau risque de niveau 2 ou un risque de niveau 1 réévalué au niveau 2 | | Analyse de risque à jour | Nouveau risque identifié de niveau 2 | RSSI | Centre Expert SSI |
| 24 | Informer l'AH<br>(AR + Plan d' Amélioration Continu de la Sécurité) | | Analyse de risque à jour et Plan d' Amélioration Continu de la Sécurité | | RSSI | Centre Expert SSI |
| 25 | Identifier un nouveau risque de niveau 3 ou un risque de niveau inférieur réévalué au niveau 3 | | Analyse de risque à jour | Nouveau risque identifié de niveau 3 | RSSI | Centre Expert SSI |
| 26 | Présenter risque(s) en Commission d'Homologation sur dossier ou formelle | Le choix est effectué par le Centre Expert SSI en fonction du contexte : prévoir d'organiser GT SSI | Dossier d'homologation | Avis du Centre Expert SSI | RSSI | Centre Expert SSI |
| 27 | Identifier un nouveau risque de niveau 4 ou un risque de niveau inférieur réévalué au niveau 4 | | Analyse de risque à jour | Nouveau risque identifié de niveau 4 | RSSI | Centre Expert SSI |
| 28 | Présenter risque(s) en Commission d'Homologation formelle | | Dossier d'homologation | Avis du Centre Expert SSI | RSSI | Centre Expert SSI |
| 29 | Statuer sur l'homologation | Homologation acceptée ou refusée avec plan d'actions plus ou moins conséquent | Avis du Centre Expert SSI | Plan d'actions | AH | Centre Expert SSI |
| 30 | Mettre à jour le tableau de bord de suivi de la dette SSI en traçant son origine | Plan d'amélioration continu de la SSI cadencé (RSSI-P)<br>Origines possibles de la dette SSI :<br>- conformité réglementaire<br>- risque métier (Plan d'Amélioration Continu de la Sécurité EBIOS RM)<br>- conformité NFR<br>- abrasion conception produit ou contractuelle (rupture ou sens large)<br>- vulnérabilité (CVE) ou défaut de MAJ engendrant une indisponibilité (MCO pur)<br>- conformité guide durcissement (<hardening>)<br>- désactivation des services inutiles (tracer les mesures organisationnelles de contournement)<br>- plan d'actions CoH (Commission d'Homologation)<br>- plan d'actions suite à audit(s) | | | RSSI | Centre Expert SSI |

# 4 Suivi des versions

| Version | Date | Commentaires |
|---|---|---|
| V1 | 28/10/2022 | Version initiale |
| | | |