L'HOMOLOGATION DE SECURITE

Documents types

Table des matières

Objectifs de ce guide 4
PARTIE 1 : Définition de la stratégie d'homologation 5
Stratégie d'homologation 6
PARTIE 2 : Maîtrise des risques 8
Analyse des risques 9
FEROS 11
PDS 13
Plan d'action 16
Risques résiduels 16
PES 18
PARTIE 3 : Prise de décision 21
Avis de la commission d'homologation 22
sur l'homologation du SI 22
Décision d'homologation du SI 23
GLOSSAIRE et DEFINITIONS 25

Objectifs de ce guide

Ce document a pour but de compléter le *guide d'homologation en neuf étapes simples* en fournissant les sommaires types des principaux documents qui doivent constituer le dossier d'homologation (étape 4 du guide).

Il s'appuie sur l'annexe 3 du guide, en ne détaillant que les documents qui doivent être établis.

Comme tous les modèles, ces sommaires-types devront être adaptés au cas d'espèce. En particulier, suivant la taille et la complexité du système d'information qui fait l'objet de l'homologation, il conviendra d'adapter le nombre d'acteurs et de rôles à impliquer, ainsi que le nombre de documents à produire et le degré de précision de leur contenu.

<table>
<tr><th></th><th>Pianissimo</th><th>Mezzo Piano</th><th>Mezzo Forte</th></tr>
<tr><td>Stratégie d'homologation</td><td colspan="3">Indispensable</td></tr>
<tr><td>Référentiel de sécurité</td><td colspan="3">Si existant</td></tr>
<tr><td>Document présentant les risques identifiés et les objectifs de sécurité</td><td colspan="3">Indispensable</td></tr>
<tr><td>Procédures d'exploitation sécurisée du système</td><td colspan="3">Indispensable</td></tr>
<tr><td>Journal de bord de l'homologation</td><td colspan="3">Fortement recommandé</td></tr>
<tr><td>Certificats de qualification des produits ou prestataires</td><td colspan="3">Si existant</td></tr>
<tr><td>Résultats d'audits</td><td>Si existant</td><td>Recommandé</td><td>Fortement recommandé</td></tr>
<tr><td>Décision d'homologation</td><td colspan="3">Indispensable</td></tr>
<tr><td colspan="4">Spécifiquement pour les systèmes déjà en service :</td></tr>
<tr><td>Tableau de bord des incidents et de leur résolution</td><td colspan="3">Indispensable</td></tr>
<tr><td>Résultats d'audits intermédiaires</td><td>Si existant</td><td colspan="2">Recommandé</td></tr>
<tr><td>Journal des évolutions du système</td><td colspan="3">Si existant</td></tr>
</table>

PARTIE 1 : Définition de la stratégie d'homologation

Le RSSI formalise l'organisation de l'homologation dans un document de synthèse validé par l'autorité d'homologation. Cette **stratégie d'homologation** précise l'ensemble des parties prenantes à l'homologation ainsi que :

- le cadre réglementaire applicable (règles de protection des informations confidentielles, règles sectorielles, etc.) ;
- l'organisation (acteurs, missions, etc.) ;
- la démarche ;
- le périmètre et le cycle de vie du SI à homologuer ;
- le calendrier ;
- la criticité des informations utilisées dans le cadre de l'homologation ;
- les pièces constitutives du dossier d'homologation.

Stratégie d'homologation

Sommaire Type

1. PRINCIPES GENERAUX

Homologation

Textes applicables (réglementation nationale, réglementation internationale)

Référentiel interne

2. DEMARCHE D'HOMOLOGATION

Application du principe général

Homologation initiale

Renouvellement de l'homologation

3. PRESENTATION GENERALE DU SYSTEME

Objet et contexte d'utilisation du SI

Périmètre technique du SI (le ou les systèmes)

Interconnexion du SI

Périmètre physique du SI (le ou les sites)

Architecture globale

Durée de validité du SI (besoin pour une phase de test, d'exercice, de mission ou de fonctionnement nominal)

4. BESOINS DE SECURITE DU SI

Reprendre ici de façon synthétique les résultats de l'analyse des besoins de sécu du SI, notamment en termes de DIC

5. ACTEURS ET RESPONSABILITES

Autorité administrative (AA) / Autorité d'emploi (AE)

Rôles possibles : HFDS/FSSI

Autorité qualifiée (AQ)

Rôles possibles : ASSI/OSSI/RSSI

Autorité d'homologation (AH)

Commission d'homologation (CH)

Responsabilités de la commission d'homologation

Composition de la commission d'homologation

Réunion(s) de la commission d'homologation

Groupe de travail pour la SSI (GTSSI)

Autorité d'Exploitation

Rôles possibles : RSSI, Administrateur-SI/Réseau

Représentants des utilisateurs

Phase d'exploitation

6. PERIMETRE D'HOMOLOGATION

Dossier d'homologation

Pièces principales rédigées en amont du cycle SSI

Pièces SSI du dossier d'homologation

7. AUDITS ET CONTROLES DE SECURITE

Présentation de la démarche

Besoins en amont, pendant et en aval des audits sur site

Planning des interventions

8. MCS

Présentation générale

Gestion de configuration

9. CYCLE DE VIE DU SI

Planning global du SI

Développement / installation

Mise en service opérationnel (MSO)

Maintien en condition de sécurité (MCS)

Maintien en condition opérationnelle (MCO)

Retrait de service

Planning global de l'homologation

Saisine de l'autorité d'homologation

Commission d'homologation

Décision d'homologation

10. GLOSSAIRE

PARTIE 2 : Maîtrise des risques

Cette partie permet à la maitrise d'œuvre (MOE), au RSSI ou au prestataire extérieur, à l'issue d'une **analyse de risques** réalisée selon une méthode respectant si possible la norme ISO 27005, d'élaborer cinq documents afin de décrire :

- les besoins et les objectifs de sécurité du système, en termes de disponibilité, d'intégrité et de confidentialité par rapport aux menaces identifiées. Au besoin, ce document peut être présenté sous la forme d'une ***fiche d'expression rationnelle des objectifs de sécurité*** (**FEROS**) ;
- les mesures de sécurité envisagées pour répondre aux objectifs de sécurité, qui peuvent être formalisées dans un **plan de sécurité (PDS)** ;
- les mesures de sécurité à mettre en place, sous la forme d'un **plan d'action** désignant les différents responsables des actions;
- les vulnérabilités résiduelles, constatées lors des audits et/ou des tests et non corrigées, ainsi que les plans d'actions associés, présentés dans un **tableau de risques résiduels** ;
- les mesures de sécurité permettant de répondre aux objectifs de sécurité fixés par l'autorité d'homologation, décrites dans les **procédures d'exploitation de sécurité (PES)**. Ces mesures présentent les droits et les devoirs des accédants au système, ainsi que les actions à réaliser dans le cadre de l'utilisation quotidienne du système.

Analyse des risques

Sommaire type

1. ÉTUDE DES RISQUES

ÉTUDE DU CONTEXTE

Le cadre de la gestion des risques

Les métriques utilisées

Les biens identifiés

ÉTUDE DES EVENEMENTS REDOUTES

Événements redoutés

Évaluation des événements

ÉTUDE DES SCENARIOS DE MENACES / MENACES

Scénarios de menaces

Évaluation des scénarios de menaces

ÉTUDE DES RISQUES

Les risques

Évaluation des risques

Les objectifs de sécurité

ÉTUDE DES MESURES DE SECURITE

Les mesures de sécurité : une défense en profondeur pour réduire les risques

Risques résiduels

Plan d'action

Homologation de sécurité

2. LIVRABLES EMANANT DE L'ETUDE EBIOS

Fiche d'expression rationnelle des objectifs de sécurité (FEROS)

Politique de sécurité (PSSI)

Dossier des risques résiduels

Décision d'homologation

3. ANNEXE : LISTE DETAILLEE DES SCENARII DE MENACES

FEROS

Sommaire Type

1. INTRODUCTION

Contexte général
Définition des responsabilités
Agrément, caution ou certificat
Evaluation
Homologation
Relations entre la FEROS et les autres documents du projet
Interconnexions de systèmes

2. DESCRIPTION DU SYSTEME

Enjeux et missions du système
Architecture du système-cible
Etats et modes d'exploitation
Cycle de vie
Mode d'exploitation de la sécurité
Biens essentiels
Fonctions du système
Informations du système
Description fonctionnelle
Fonction 1
Fonction 2
Fonction *n*
Environnement du système
Locaux d'implantation
Personnel intervenant sur le système

3. CONTRAINTES ET HYPOTHESES

Contraintes
Hypothèses

4. BESOINS DE SECURITE

Critères de sensibilité

Echelle de sensibilité

Besoins de sécurité

5. ETUDE DES MENACES

Origine des menaces : éléments menaçants

Niveaux de menaces

Eléments menaçants

Motivations

Menaces retenues

Impacts

6. LES EVENEMENTS REDOUTES

Echelle de cotation des probabilités

Evènements redoutés

7. LES RISQUES

Evènement inacceptable

8. LES OBJECTIFS DE SECURITE

Couverture des risques par les objectifs

9. RISQUES RESIDUELS

10. COMPLEMENTS

Réglementation générale

Réglementation spécifique

Documents de référence

Glossaire

Abréviations

ANNEXE A : SYNOPTIQUE DE LA METHODE

ANNEXE B PROCESSUS D'ANALYSE DES RISQUES

Identification des risques d'après les évènements redoutés (ER)

Inventaire des ER

Elaboration des arbres d'attaque et de défaillance

PDS

Sommaire type

1. INTRODUCTION

Objet : Plan de Sécurité et spécification SSI du système

Organisation du document

Documents à appliquer et documents de référence

Documents à appliquer

Documents de Référence

Normes/Standards

Autres documents

Terminologie

Sigles et abréviations

Glossaire

2. PRESENTATION DU SI

Contexte général

Définition et levée de risques et décision de lancement de la réalisation

Définition et levée de risques SSI

Projet de PDS

3. PERIMETRE DE L'ETUDE

Liste des données sensibles

Flux de données

Hypothèses prises en compte

4. PRESENTATION DE L'ARCHITECTURE EXISTANTE

Architecture des SI de même type

Architecture du SI

Les interconnexions

5. BESOINS DE SECURITE DU SI

Présentation générale des besoins de sécurité

Besoins de sécurité

Besoins génériques du SI

Besoin de sécurité vis à vis des systèmes interconnectés

Besoin de sécurité des informations nationales vis à vis des organismes extérieurs

Les objets sensibles

Les types d'objets sensibles

Besoins de sécurité « DIC » des données et fonctions sensibles

Besoins consolides

6. POLITIQUE DE SECURITE DU SI

Politique de sécurité non-technique

Mesures générales liées à l'organisation et au contrôle de la sécurité

Mesures de sécurité liées à l'information

Mesures de sécurité des biens physiques

Mesures liées à la sécurité du personnel

Mesures de sécurité liées au cycle de vie du système

Politique de sécurité technique

7. CONFORMITE AUX OBJECTIFS ET EXIGENCES DE SECURITE

TEMPEST

Description des solutions envisagées pour la protection contre les SPC

Les solutions pour la protection contre les SPC

Conformité aux exigences sur la protection contre les SPC

Protection physique

Description des solutions de protection physique

Conformité aux objectifs de sécurité sur la protection physique

Identification, authentification et contrôle d'accès

Description des solutions identification et authentification envisagées

Conformité aux exigences relatives aux fonctions d'identification, d'authentification et de contrôle d'accès logique

Gestion du multi-contexte

Solutions envisagées pour l'effacement d'urgence

Solution envisagée pour l'effacement des mémoires volatiles

Solution envisagée pour la désactivation des fonctions d'enregistrement

Solutions envisagées pour l'effacement des mémoires non volatiles

Solutions envisagées pour le chiffrement des données

Procédures de maintenance

Solutions pour la gestion du multi contexte

Conformité aux exigences sur la gestion multi contexte

Audit

Solution relative à l'imputabilité et aux données d'audits

Conformité aux exigences sur l'imputabilité et aux données d'audits

Mécanismes de contrôle d'émissions (EMCON)

Solutions de contrôle d'émissions

Conformité aux exigences sur le contrôle des émissions

Interconnexion du SI

Solutions relatives à l'interconnexion du SI

Conformité aux exigences sur l'interconnexion des systèmes

Intégrité des données et logiciels

Solutions envisagées pour assurer l'intégrité et la maintenance des données

Solutions relatives à l'intégrité des données, des logiciels et la gestion de la configuration

Conformité aux exigences sur l'intégrité des données, des logiciels et la gestion de la configuration

Communications

Solutions de sécurité sur le système de communication

Conformité aux exigences sur les systèmes de communications

Conformité aux autres exigences

Matrice de conformité

Plan d'action

Exemple de tableau de suivi du plan d'action :

Actions	Responsable	Difficulté	Coût financier	Terme	Avancement
Action-1					
Action-2					

Exemple d'échelle utilisable :

Difficulté	Coût financier	Terme	Avancement
1. Faible	1. Nul	1. Trimestre	1. Non démarré
2. Moyenne	2. Moins de 1 000€	2. Année	2. En cours
3. Élevée	3. Plus de 1 000€	3. Trois ans	3. Terminé

Risques résiduels

Exemple de présentation :

N° Risque Résiduel	**N° Mesure de sécurité impactée**	**Risque Résiduel Préliminaire identifié avant la mise en œuvre complète des PASSI**	**Vulnérabilité**	G	V	Niveau du Risque	Réduction du risque proposée
					1		

Exemple de métrique :

Echelle de gravité		
Niveau	**Echelle**	**Description**
1	**Négligeable**	Les impacts peuvent être surmontés sans difficultés
2	**Limitée**	Les impacts peuvent être surmontés avec quelques difficultés
3	**Importante**	Les impacts peuvent être surmontés avec de sérieuses difficultés
4	**Critique**	Les impacts sont potentiellement insurmontables

Echelle de vraisemblance		
Niveau	**Echelle**	**Description**
1	**Minime**	Cela ne devrait pas se produire
2	**Significative**	Cela pourrait se produire
3	**Forte**	Cela devrait se produire un jour ou l'autre
4	**Maximale**	Cela va certainement se produire prochainement

Critères d'évaluation des risques

gravité	4	Intolérable	Intolérable	Intolérable	Intolérable
	3	Significatif	Significatif	Intolérable	Intolérable
	2	Négligeable	Négligeable	Significatif	Intolérable
	1	Négligeable	Négligeable	Négligeable	Négligeable
		1	2	3	4
		Vraisemblance			

PES

Sommaire type

1. ADMINISTRATION ET ORGANISATION DE LA SECURITE

Introduction

Documents de référence

Description du système

Historique et vue d'ensemble

Description du système

Mode d'exploitation

Accréditation

Responsabilités

Autorité de sécurité

OSSI

Administrateurs

Utilisateurs

Diffusion des SecOPs

Gestion des utilisateurs et de leurs droits

Signalement des incidents de sécurité

Procédures de contrôle applicables aux supports amovibles ou matériels privés

Sécurité des télécommunications

2. SECURITE PHYSIQUE

Identification des zones sensibles

Emplacements des équipements

Gestion des clés et des combinaisons

Contrôle d'accès

Contrôle des équipements

Gestion des alarmes et de la sécurité

Sécurité physique en dehors des heures de travail

3. SECURITE DES PERSONNES

Liste du personnel

Habilitations

Formation à la sécurité

Liste des accès autorisés

Personnel de maintenance et d'entretien

4. SECURITE DES DOCUMENTS

Identification des documents

Inspections d'enregistrements et responsabilités

Contrôle, stockage et marquage des documents

Création, diffusion et réception de documents

Contrôle des enregistrements

Gestion des supports informatiques

Déclassification et destruction

5. SECURITE DU SI

Environnement système

Environnement matériel

Arrêt / démarrage des machines

Connexion et déconnexion de matériels

Contrôles d'intégrité matérielle

Maintenance du système

Sécurité du logiciel

Contrôle d'accès au système informatique

Gestion des comptes utilisateurs

Contrôle lors de l'installation de logiciels

Masterisation logicielle et copies de sauvegarde

Gestion des traces d'audit

Archivage des journaux d'audit

Protection contre les virus

Zonage TEMPEST

Gestion des équipements chiffre et des clés associées

Gestion des filtres de sécurité

6. PLAN DE SECOURS

Sauvegarde systèmes et sauvegarde des données utilisateurs

Stockage et accès aux supports de sauvegarde

Reprise sur incident matériel

Gestion des pertes d'alimentation électrique

Climatisation

Gestion des pertes de moyen de télécommunication

Protection incendie

Mesures d'urgence

7. GESTION DE CONFIGURATION

Responsabilités pour la gestion de configuration

Configuration de référence

Gestion des évolutions matérielles & logicielles

8. ANNEXES

A. Missions de responsabilités de l'OSSI

B. Misions et responsabilités des administrateurs du SI

C. Liste des personnels

PARTIE 3 : Prise de décision

Lors de la commission d'homologation, les différents acteurs analysent les risques résiduels afin de pouvoir émettre un avis sur la décision d'homologation. Cet avis est porté à la connaissance de l'autorité d'homologation et lui permet de décider en connaissance de cause.

Avis de la commission d'homologation sur l'homologation du SI

Sommaire type

1. CONTEXTE

Contexte du dossier d'homologation

Cadre réglementaire applicable

Référence à la note de mise en place de la commission d'homologation

2. PRESENTATION DU SI

Enjeux et missions du SI

Besoins de sécurité

Architecture du SI cible

Interconnexions

Sites de déploiement

Planning

3. ANALYSE DU DOSSIER

4. AVIS DE LA CH

Compte rendu de la CH

Avis de la CH

Décision d'homologation du SI

Sommaire type

1. CONTEXTE

Contexte du dossier d'homologation

Cadre réglementaire applicable

2. PRESENTATION DU SI

Enjeux et missions du SI

Besoins de sécurité

Architecture du SI cible

Interconnexions

Sites de déploiement

Planning

3. DECISION D'HOMOLOGATION

Le FONCTION_DE_L'AUTORITE_D'HOMOLOGATION, représentant l'autorité d'homologation désignée par REFERENCE_ET_DATE_DU_DOCUMENT

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 au niveau NIVEAU_RETENU dans la configuration présentée dans le dossier d'homologation [rappelée en annexe XXX] [et sous réserve de 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

3. Bis. 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

GLOSSAIRE et DEFINITIONS

AA	Autorité Administrative
AE	Autorité d'emploi
AH	Autorité d'homologation
AQ	Autorité qualifiée
CH	Commission d'homologation
EMCON	Mécanismes de contrôle d'émissions
ER	Evénement redouté
FEROS	Fiche d'expression rationnelle des objectifs de sécurité
GTSSI	Groupe de travail SSI
MCO	Maintien en condition opérationnelle
MCS	Maintien en condition de sécurité
MSO	Mise en service opérationnel
PDS	Plan de sécurité
PES	Procédures d'exploitation de sécurité
PSSI	Politique de sécurité des systèmes d'information
RSSI	Responsable de la sécurité des systèmes d'information
SI	Système d'information
SPC	Signaux parasites compromettants
SSI	Sécurité des systèmes d'information

Autorité d'emploi : autorité à l'origine du besoin du système d'information. Elle est également responsable de sa mise en œuvre. C'est l'autorité d'emploi qui, après avoir défini les finalités du traitement, en pilote l'emploi et les évolutions. Elle est garante de la bonne utilisation du SI. Elle pilote l'emploi et les évolutions sous couvert de l'Autorité d'homologation.

Autorité d'homologation : autorité de niveau hiérarchique suffisant, désignée par l'Autorité qualifiée SSI. Sur avis de la commission d'homologation, elle signe la décision autorisant l'emploi d'un système d'information. Cette compétence en matière d'homologation peut être déléguée à une autorité déléguée. La délégation fixe alors les limites des attributions correspondantes et précise le niveau maximal de confidentialité pour lequel chaque autorité déléguée est compétente.

Autorité qualifiée SSI : Les autorités qualifiées sont responsables de la sécurité des systèmes d'information au niveau d'un service, d'une direction d'un ministère, au niveau d'un organisme ou d'un établissement relevant d'un ministère.

Les autorités qualifiées sont désignées par le ministre pour le département et les organismes dont il a la charge.

Dans le cas d'un organisme qui ne relève pas d'un ministre, notamment un organisme privé, il appartient au responsable de cet organisme de désigner, en son sein, une personne ayant la fonction d'autorité qualifiée.

Fonctionnaire de Sécurité des Systèmes d'Information (FSSI) : agent chargé de s'assurer de la bonne exécution des directives et des orientations ministérielles et interministérielles ainsi que de la coordination et de la cohérence des actions menées dans le ministère. A ce titre, il veille à la conformité des démarches d'homologation de sécurité du SI avec la politique de sécurité des systèmes d'information du ministère. Le FSSI est membre de droit de la commission d'homologation et peut se faire représenter aux différentes commissions d'homologation de sécurité.

Mise en service opérationnel (MSO) : décision qui formalise l'autorisation d'emploi opérationnel par l'autorité cliente. L'une des conditions sur lesquelles repose cette prise de décision est l'homologation préalable du système

Responsable de la sécurité des système d'information (RSSI) : personne chargée de faire appliquer la politique SSI interne du système, en conformité avec la politique SSI de l'organisme

Version 1.0 – Juin 2015

20150327-1158

AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION

ANSSI – 51, boulevard de la Tour-Maubourg – 75700 PARIS 07 SP

www.ssi.gouv.fr / communication@ssi.gouv.fr