Annexe D

Guide d'homologation de sécurité d'un téléservice

Historique des versions		
Date	Version	Évolution du document
18/10/2018	1.0	Publication de la première version de l'annexe D du Référentiel Général de Sécurité (RGS PF)

Avant-propos

Ce guide d'homologation s'adresse à l'ensemble des autorités administratives visées au 1° de l'article 1er de la loi du Pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices, à savoir : la Polynésie française, ses établissements publics, les autorités administratives indépendantes, les organismes de protection sociale et les autres organismes et personnes de droit public et de droit privé chargés d'une mission de service public administratif.

Pourquoi l'homologation de sécurité ?

Lorsqu'un responsable (autorité administrative, élu, dirigeant d'entreprise) décide de faire déménager ses équipes dans de nouveaux locaux ou d'ouvrir un établissement recevant du public, il s'assure que les lieux sont conformes à la réglementation et que les bâtiments sont solides, afin que l'ensemble puisse fonctionner en toute sécurité pour les personnes et les biens. Il doit s'en assurer même s'il n'est pas un spécialiste de la construction et il s'appuie pour cela sur des garanties et des arguments portés à sa connaissance par des experts du domaine. Ce responsable atteste par sa décision d'homologation que ses locaux sont conformes à la réglementation en vigueur, que les risques liés au bâtiment et à son exploitation sont identifiés et maitrisés. Le responsable supportera les éventuelles conséquences juridiques d'une homologation.

En matière de services informatiques et plus particulièrement dans ceux ouverts sur l'Internet, l'homologation de sécurité joue le même rôle. Elle permet à un responsable, en s'appuyant sur l'avis d'experts, d'identifier et d'attester aux utilisateurs d'un système d'information que les risques qui pèsent sur eux, sur les informations qu'ils manipulent et sur les services rendus, sont connus et maîtrisés. L'homologation est d'autant plus nécessaire, aujourd'hui, que les systèmes d'information sont de plus en plus complexes et ouverts et que les impacts potentiels d'un incident sont de plus en plus graves. Les cyber attaques vers les systèmes informatiques dont de plus en plus nombreuses. Les atteintes aux systèmes d'information (SI) d'une organisation deviennent bloquantes, perturbantes et souvent couteuses. L'ouverture d'un SI d'une autorité administrative doit donc être prêt aux atteintes des cybercriminels comme aux erreurs ou malveillances internes.

Une démarche d'homologation est donc un préalable à l'instauration de la confiance dans les systèmes d'information et dans leur exploitation. **Sa prononciation par le responsable de l'organisation ou Autorité d'Homologation, est un préalable à l'ouverture du SI ou du Téléservice**.

Pour un certain nombre de systèmes, l'homologation est rendue obligatoire par la loi du pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices. Cette réglementation vise à préciser les dispositions de mise en œuvre de la sécurité des systèmes d'informations d'une autorité administrative, notamment lorsque celle-ci met à disposition des téléservices. Le cadre technique et organisationnel de cette sécurité est le Référentiel Général de Sécurité (RGS) de la Polynésie française.

Ce guide d'homologation RGS est inspiré du Guide d'homologation de sécurité en neuf étapes (version 1.0 - Août 2014), rédigé par l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI). Il peut s'appliquer pour toute autre exigence réglementaire prévue par la Polynésie française.

Qu'est-ce qu'une homologation de sécurité ?

En informatique, comme dans les autres domaines, le risque zéro n'existe pas. La démarche d'homologation de sécurité est destinée à faire connaître et faire comprendre aux responsables les risques liés à l'exploitation d'un système d'information, notamment ceux liés à la cybersécurité

Il s'agit d'un processus d'information et de responsabilisation qui aboutit à une décision, prise par le responsable de l'organisation. Cette décision constitue un acte formel par lequel le responsable :

- atteste de sa connaissance du système d'information et des mesures de sécurité (techniques, organisationnelles ou juridiques) mises en œuvre ;
- accepte les risques qui demeurent, qu'on appelle risques résiduels.

La décision s'appuie sur l'ensemble des documents que le responsable estime nécessaire et suffisant à sa prise de décision.

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

- dans les cas de systèmes complexes ou à fort enjeu de sécurité de l'information ou de cybersécurité, il est souhaitable que le responsable s'entoure d'experts techniques et fonctionnels : la Commission d'Homologation complète ;
- dans le cas de systèmes simples moins exposés car moins ouverts sur l'Internet, le responsable peut mettre en place des procédures simplifiées associant un nombre plus limité d'acteurs dans une Commission d'Homologation réduite.

Comment homologuer un système d'information ?

La démarche d'homologation est décomposée en neuf étapes. Chacune de ces étapes est décrite ci-après. La démarche proposée est inspirée de l'approche ouverte de l'ANSSI, mais la Polynésie française a fixé des éléments et pris des options dans son processus d'homologation.

Pour chacune des étapes, le présent guide décrit les actions attendues, les responsables, les acteurs et les livrables attendus pour le déroulement de l'étape et ceux produits par l'étape.

Les étapes d'homologation de sécurité d'un téléservice sont les suivantes:

1. Identification et description du contexte du téléservice
2. Détermination de la démarche d'homologation au regard des enjeux de sécurité
3. Définition de la gouvernance de l'homologation
4. Elaboration du dossier d'homologation et du planning
5. Réalisation de l'analyse des risques du téléservice
6. Evaluation et amélioration du niveau de sécurité du téléservice
7. Mesures de sécurité complémentaires pour couvrir les derniers risques
8. Décision d'homologation du téléservice
9. Surveillance des risques résiduels du téléservice

Table des matières

Objectifs de l'homologation de sécurité

En informatique, comme dans les autres domaines, le *risque zéro* n'existe pas.

L'objectif de la *démarche d'homologation* d'un système d'information (SI) est de trouver un équilibre entre le risque acceptable et les coûts de sécurisation, puis de faire arbitrer cet équilibre, de manière formelle, par un responsable qui a autorité pour le faire.

Cette démarche permet d'améliorer la sécurité pour un coût optimal, en évitant la « sur-sécurité », mais en prenant également en compte le coût d'un éventuel incident de sécurité. L'approche permet de s'assurer que les risques pesant sur un système d'information précis (le périmètre de l'homologation), dans son contexte d'utilisation, sont connus et maîtrisés de manière active, préventive et continue.

La démarche d'homologation est intégrée au cycle de vie du système d'information. Elle comprend neuf étapes clés, détaillées au sein du présent document. Il est nécessaire de les suivre en même temps que les phases de développement du système : opportunité, faisabilité, conception, réalisation, validation, exploitation, maintenance et fin de vie.

A quel moment entrer dans ce processus d'homologation ?

La présente démarche d'homologation doit être activée à des moments clés de la vie d'un projet de téléservice :

- Lors du lancement d'un nouveau projet de téléservice par le Responsable, afin de comprendre le plus tôt possible les enjeux de sécurité pour adapter le processus d'homologation. Ce dernier accompagnera le projet tout au long de son cycle de vie ;
- À tout moment, si la démarche d'homologation formelle n'était pas disponible au moment de la mise en production du téléservice.

Attention, la Loi de Pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices fixe les délais dans lesquels un Téléservice doit être homologué.

La *décision d'homologation* par l'Autorité d'Homologation est le résultat du processus. Son objet est de vérifier que le responsable a analysé les risques de sécurité et a mis en œuvre les dispositifs adaptés à la menace.

Le terme « homologation » recouvre donc deux notions distinctes :

- la démarche d'homologation, avant tout destinée à faire connaître et faire comprendre aux responsables les risques liés à l'exploitation d'un système d'information. Elle se conclut par une décision, soutenue par la constitution et l'analyse d'un dossier de sécurité ;
- la décision formelle d'homologation (également appelée attestation formelle).

Se lancer dans une démarche d'homologation est relativement simple : il s'agit de vérifier que la sécurité n'a pas été oubliée avant la mise en place du téléservice et d'appliquer les mesures de sécurité nécessaires et proportionnées.

Les neuf étapes simples présentées dans ce document permettront à un chef de projet ou à un comité de pilotage SSI de préparer un dossier d'homologation et de le présenter au responsable de l'organisation, désigné *autorité d'homologation*.

L'autorité d'homologation pourra alors prendre une décision éclairée sur la base de ce dossier, qui doit apporter des réponses pertinentes à l'ensemble des questions qu'elle se pose.

Dans la suite du document :

- les documents attendus sont les documents et informations nécessaires pour lancer le processus, l'étape. Ce sont les documents d'entrée de l'étape.
- les livrables sont les documents formalisés à l'issu du processus, de l'étape. Ce sont les documents de sortie de l'étape.

Etape 1 : Identification et description du contexte du téléservice

Document(s) attendu(s) :

- Tous documents permettant de délimiter le périmètre du système (cahier des charges, étude préalable…)

Participants potentiels à l'Étape 1 :

- Responsables métiers ;
- Assistance à maîtrise d'ouvrage ;
- Experts techniques internes ;

1. Délimiter le périmètre du système

Le périmètre du téléservice 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 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.

Livrable(s) produit(s) :

- Compte rendu de la réunion lors de laquelle le téléservice a été décrit dans un périmètre donné.

Etape 2 : Détermination de la démarche d'homologation au regard des enjeux de sécurité

Durant cette deuxième étape, vous définissez le niveau de profondeur de la démarche d'homologation, afin que celle-ci soit adaptée aux enjeux de sécurité du téléservice, d'une part, et aux capacités de votre organisme à la mener, d'autre part.

La démarche la plus adaptée à l'homologation du système doit être définie en fonction du contexte, du niveau de complexité et de criticité du système, du niveau de sensibilité des données hébergées (notamment si le téléservice collecte ou traite des données à caractère personnel) et du niveau de maturité en matière de SSI de l'organisme qui met en œuvre l'homologation.

Document(s) attendu(s) :

- Les outils d'autodiagnostic pour l'évaluation des besoins de sécurité du téléservice et de maturité de l'organisme.

Participants potentiels à l'Étape 2 :

- Responsables métiers ;
- Assistance à maîtrise d'ouvrage ;
- Experts techniques internes ;
- RSSI

1. Réaliser l'autodiagnostic des besoins de sécurité du téléservice et le niveau de maturité SSI de l'organisme

Deux outils d'autodiagnostic sont proposés. Ils sont détaillés en annexe du présent document.

L'annexe 1 permet d'évaluer les besoins de sécurité du téléservice à homologuer,

- En estimant la gravité des conséquences potentielles d'une défaillance du SI, la sensibilité des données, le degré d'exposition aux menaces et l'importance des vulnérabilités potentielles du système,
- Un questionnaire simple et rapide permet de déterminer si le besoin de sécurité du système est nul, faible, moyen ou fort.
- L'annexe 2 permet de déterminer votre niveau de maturité SSI,
- C'est-à-dire le niveau de maîtrise et de rigueur atteint par l'organisme, dans la gestion de la sécurité des systèmes d'information,
- Un questionnaire simple et rapide vous permet de déterminer si la maturité SSI de votre organisme est élémentaire, moyenne ou avancée.

2. En déduire la démarche appropriée

En fonction des résultats de l'autodiagnostic des besoins de sécurité et du niveau de maturité, vous pouvez déterminer, à l'aide du tableau ci-dessous, le type de démarche d'homologation à mettre en œuvre dans le cadre de votre projet de téléservice.

Les autodiagnostics doivent être réalisés avec sérieux et objectivité. L'adoption d'une démarche inadaptée aux enjeux ou aux capacités de votre organisme hypothèquerait les chances de réussite de votre projet d'homologation.

		Besoin de sécurité du système		
		Faible	Moyen	Fort
Niveau SSI de l'organisation	Elémentaire	Simple	Avancée	Avancée
	Moyen	Simple	Avancée	Détaillée
	Avancé	Simple	Avancée	Détaillée

Les démarches possibles sont les suivantes :

- **Simple :** démarche autonome à minima, que la Commission d'homologation peut mener sans recours à une assistance conseil externe, par l'application des outils et des indications donnés dans le présent guide,
- **Avancée :** démarche autonome approfondie, que la Commission d'homologation peut mener sans recours à une assistance conseil externe, par l'application des outils et des indications donnés dans le présent guide et ses ressources internes,
- **Détaillée :** démarche assistée approfondie, que la Commission d'homologation mène avec l'aide d'une assistance conseil externe, en plus des outils et des indications données dans le présent guide.

Livrable(s) produit(s) :

- Compte rendu de la réunion lors de laquelle le niveau de profondeur de la démarche d'homologation a été retenu et validé.

Etape 3 : Définition de la gouvernance de l'homologation

Durant cette troisième étape, vous identifiez l'ensemble des acteurs de l'homologation et définir leur rôle (décision, assistance ou expertise technique notamment).

Une homologation s'appuie sur plusieurs acteurs distincts auxquels sont associés différents rôles et niveaux de responsabilité.

Document(s) attendu(s) :

- Aucun document n'est nécessaire pour lancer cette étape.

Participants potentiels à l'Étape 3 :

- Autorité d'homologation
- Responsables métiers ;
- Assistance à maîtrise d'ouvrage ;
- RSSI ;

1. L'autorité d'homologation (AH)

L'autorité d'homologation est la personne physique qui, après instruction du dossier d'homologation, prononce l'homologation de sécurité du téléservice, c'est-à-dire prend la décision d'accepter les risques résiduels identifiés sur le système.

L'autorité d'homologation doit être désignée à un niveau hiérarchique suffisant pour assumer toutes les responsabilités. Il est donc nécessaire que l'autorité d'homologation se situe à un niveau de direction dans votre organisme.

Pour la Polynésie française, l'autorité d'homologation est le Président de la Polynésie française. Ce dernier peut déléguer cette compétence au vice-président et aux ministres du gouvernement de la Polynésie française.

L'autorité d'homologation désigne un responsable du processus d'homologation, qui mènera le projet d'homologation en son nom.

Lorsque cela est nécessaire, l'autorité d'homologation peut rédiger une lettre de mission à l'attention de la personne chargée d'organiser les tâches du processus d'homologation, en lui indiquant de quelle manière la synthèse des résultats de chaque étape de la démarche d'homologation lui sera communiquée.

Lorsque le système est sous la responsabilité de plusieurs autorités, l'autorité d'homologation est désignée conjointement par les autorités concernées

2. La 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.

La taille et la composition de cette commission doivent être adaptées à la nature du téléservice et proportionnées à ses enjeux, en particulier si ce dernier est très sensible, notamment dans le cas d'un téléservice manipulant des données à caractère personnel sensibles.

- La commission est dite **complète** quand elle est composée de :
  - Responsables métiers ;
  - Assistance à maîtrise d'ouvrage ;
  - Experts techniques internes ;
  - Responsable de la production informatique ;
  - RSSI ;
  - Correspondant Informatique et Libertés (CIL) ou Délégué à la Protection des Données (DPO) si le Téléservice manipule des données à caractère personnel.
- La commission est dite **réduite** quand elle est composée de :
  - Responsables métiers ou l'assistance à maîtrise d'ouvrage ;
  - Responsable de la production informatique ;
  - RSSI ;
  - Correspondant Informatique et Libertés (CIL) ou Délégué à la Protection des Données (DPO) si le Téléservice manipule des données à caractère personnel.

La commission d'homologation est chargée du suivi des *plannings*, de l'analyse de l'ensemble des documents versés au dossier d'homologation. Elle se prononce sur la pertinence des livrables et peut les valider dans certains cas.

Si la qualité ou la complétude des documents attendus ne satisfait pas la commission d'homologation, cette dernière peut commander en interne ou en externe des travaux complémentaires sur ces documents.

Le service informatique de la Polynésie française assiste la commission d'homologation dans l'élaboration des documents constituant le dossier d'homologation. Ce dernier assure le secrétariat de la commission d'homologation.

3. Les acteurs de l'homologation

La maîtrise d'ouvrage

La maîtrise d'ouvrage représente les acteurs métier et assure la bonne prise en compte des contraintes liées à l'utilisation du téléservice. Elle joue un rôle-clé dans plusieurs étapes de la maîtrise des risques, y compris dans les arbitrages sur le traitement des risques.

Le RSSI

Lorsque l'entité dispose d'un responsable de la sécurité des systèmes d'information, celui-ci est impliqué nécessairement dans la démarche d'homologation. Selon les cas, il peut être désigné responsable du processus d'homologation ou chargé du secrétariat de la commission d'homologation mais il est toujours membre de droit de cette commission.

Le responsable d'exploitation du système

Le responsable d'exploitation du système, ou autorité d'emploi, remplit le rôle opérationnel. Il s'agit de l'entité exploitant le système d'information destiné à être homologué.

Les prestataires

En fonction de leur statut (interne ou externe), de leur implication dans le projet et de leurs relations avec l'autorité d'homologation, les prestataires peuvent être intégrés dans la commission d'homologation, ou simplement consultés en cas de besoin.

Ils remplissent un rôle d'assistance et produisent des livrables qui seront versés au dossier d'homologation ainsi que des réponses aux interrogations de la commission d'homologation.

Les systèmes interconnectés

Les autorités d'homologation des systèmes interconnectés au système concerné peuvent jouer un rôle dans l'homologation et être associés à la démarche lorsque :

- le système à homologuer à un impact sur leurs propres systèmes ;
- ils émettent des avis ou des certificats qui peuvent concerner le système.

Le Correspondant Informatique et Libertés ou le Délégué à la Protection des Données à Caractère Personnel.

Lorsque l'organisme a désigné un **Correspondant Informatique et Libertés** ou un **Délégué à la Protection des Données à Caractère Personnel**, celui-ci est impliqué nécessairement dans la démarche d'homologation. Il apporte son expertise juridique dans le domaine à la commission d'homologation, et vérifie que les exigences relatives à la protection des données à caractère personnel sont respectées.

Livrable(s) produit(s) :

- Composition et rôle des membres de la commission d'homologation

Etape 4 : Elaboration du dossier d'homologation et du planning

Durant la quatrième étape, vous allez inventorier le contenu du dossier d'homologation et définir le planning de la démarche qui permettra de le constituer et de l'instruire.

Document(s) attendu(s) :

- Les documents attendus par la Commission d'Homologation dépendent de la démarche retenue pour l'homologation. L'objectif de cette étape est donc de fixer la qualité des documents à collecter.

Participants potentiels à l'Étape 4 :

- Commission d'homologation

1. Le contenu du dossier d'homologation

Le dossier d'homologation est alimenté pendant toutes les phases de la démarche, essentiellement avec des documents nécessaires à la conception, à la réalisation, à la validation du projet ou à la maintenance du téléservice après sa mise en service, ainsi que des documents produits spécifiquement pour l'homologation. L'annexe 3 propose une liste complète des documents qui peuvent être intégrés dans un dossier d'homologation.

Le contenu du dossier pourra varier selon la démarche choisie. Le tableau ci-dessous synthétise les éléments constitutifs du dossier d'homologation en fonction de la démarche adoptée. L'annexe 3 établit la liste plus complète des documents pouvant être contenus dans un dossier d'homologation et en propose une description détaillée.

	Démarche d'homologation (définie à l'étape 2)			
	Simple	Avancée	Détaillée	Etape
Stratégie d'homologation	Indispensable			Etape n°4
Référentiels de sécurité : • Politique de sécurité des systèmes d'information • la législation ou la réglementation particulière au contexte de l'organisme ; • le dossier de sécurité des systèmes interconnectés au système à homologuer.	Si existant			Etape n°4

Document présentant les risques identifiés et les objectifs de sécurité	Indispensable			Etape n°5
Procédures d'exploitation sécurisée du système	Indispensable			
Journal de bord de l'homologation (CRR)	Fortement recommandé			
Certificats de qualification des produits ou prestataires	Si existant			
Résultats d'audits	Si existant	Recommandé	Fortement recommandé	
Liste des risques résiduels	Indispensable			
Décision d'homologation	Indispensable			
Spécifiquement pour les systèmes déjà en service :				
Tableau de bord des incidents et de leur résolution	Recommandé	Fortement recommandé	Indispensable	
Résultats d'audits Intermédiaires	Si existant	Recommandé		
Journal des évolutions du système	Si existant			

A ces documents attendus par la commission d'homologation, d'autres documents peuvent être réclamés par cette dernière, en fonction du niveau de démarche :

- Démarche simple :

- Tous les documents décrivant les procédures de sécurité en vigueur au sein de votre organisme peuvent être intégrés au dossier, par exemple :
  - votre charte d'utilisation des postes informatiques ;
  - les règles de contrôle d'accès physique et logique au système ;
  - les clauses de sécurité des contrats de sous-traitance informatique.

- Démarche avancée ou détaillée :
  - Les documents constitutifs du référentiel de sécurité de votre organisme peuvent être intégrés au dossier. En particulier :
    - votre politique de sécurité des systèmes d'information (PSSI) ;
    - la législation ou la réglementation particulière au contexte de votre organisme ou d'un de ses secteurs d'activité ;
    - le dossier de sécurité des systèmes interconnectés au système à homologuer.
  - Votre PSSI, quand elle existe, est un document de référence pour l'homologation, car elle contient des éléments stratégiques (périmètre de sécurité, principaux besoins de sécurité et origine des menaces), ainsi que les règles en vigueur au sein de votre organisme.

L'homologation peut aussi être l'occasion de compléter (ou de rédiger) la PSSI, par exemple pour généraliser des règles indispensables au SI homologué.

Livrable(s) produit(s) :

- La validation de la collecte des documents attendus par la démarche est consignée dans le compte rendu de réunion de la commission d'homologation.

2. Planning de l'homologation

L'homologation doit être prononcée préalablement à la mise en service opérationnelle du téléservice. La Loi de Pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices fixe les délais dans lesquels un téléservice doit être homologué.

La démarche visant à l'homologation doit donc être lancée dès la phase de conception du projet puis être totalement intégrée au projet dès les phases d'étude préalable et de conception, afin d'éviter tout risque calendaire.

Le calendrier de l'homologation est directement dépendant du calendrier du projet dont il doit tenir compte en permanence. Les principales étapes de l'homologation sont fixées dans la stratégie d'homologation.

Il est indispensable de déterminer les tâches de chacun des acteurs de l'homologation et les formaliser dans un planning associé, reprenant les principales étapes. Au besoin, en fonction de l'évolution du projet, ces échéances peuvent être révisées, avec l'accord de l'autorité d'homologation.

Ainsi, une homologation est rythmée par deux temps forts :

- la construction du référentiel documentaire et l'analyse des risques ;
- le déploiement, l'audit, la prononciation de l'homologation et la mise en service opérationnel.

Les échéances prévues pour les différentes étapes de la démarche d'homologation devraient figurer dans le planning, par exemple :

1. Lancement de la procédure d'homologation (par exemple date de formalisation de la stratégie d'homologation) ;
2. Début et de fin de l'analyse des risques (dates des entretiens avec l'autorité) ;
3. Remise des différents documents du dossier d'homologation (cf. section suivante) ;
4. Engagements liés à d'éventuels contrats avec des prestataires impliqués dans le système (hébergeurs, fournisseurs de sous-systèmes, d'applications…) ;
5. Réunions de la commission d'homologation ;
6. Audits éventuels sur les composants du système (techniques ou organisationnels), logiciels plates-formes matérielles, interfaces réseaux ;
7. Homologation du système ;
8. Mise en service du système.

Livrable(s) produit(s) :

- La validation du planning du processus d'homologation est consignée dans le compte rendu de réunion de la commission d'homologation.

Etape 5: Réalisation de l'analyse des risques du téléservice

Durant cette cinquième étape, vous identifiez et ordonnez les risques qui pèsent sur le téléservice à homologuer. L'analyse de risques a été réalisée pendant la phase de développement du téléservice ou pas.

Document(s) attendu(s) :

- Les résultats de ou des analyses de risques réalisées dans le cadre du développement du téléservice. La ou les FEROS si le téléservice a fait l'objet d'un développement ;
- Si le processus d'analyse de risques faisait partie de la méthode de développement retenue.

Participants à l'Étape 5 :

- Responsables métiers ;
- Assistance à maîtrise d'ouvrage ;
- Experts techniques internes ;
- RSSI ;

1. L'analyse de risque

Un risque est la combinaison d'un événement redouté (susceptible d'avoir un impact négatif sur la mission de l'entité) et d'un scénario de menaces. On mesure le niveau du risque en fonction de sa gravité (hauteur des impacts) et de sa vraisemblance (possibilité qu'il se réalise).

Il s'agit d'identifier les risques pesant sur la sécurité du téléservice, de les hiérarchiser et de déterminer des objectifs généraux qui permettront de diminuer certains d'entre eux et, à terme, de les amener à un niveau acceptable.

La durée et le coût de la réalisation d'une analyse des risques sont fonction de la complexité du système d'information et de la sensibilité des données (données propres ou données de tiers, telles que celles des usagers ou des partenaires).

L'analyse des risques pesant sur le système peut être simplifiée dans le cadre d'une démarche Simple. Dans le cas d'une démarche Avancée ou Détaillée, on privilégiera l'utilisation d'une méthode éprouvée d'analyse des risques, comme la méthode EBIOS.

Si aucune analyse des risques n'a été menée lors de la conception du téléservice, la commission d'homologation devra commander (en interne ou en externe) une analyse des risques adaptée à la nature de la démarche d'homologation (Simple, Avancée ou Détaillée).

- Démarche Simple
  - Le tableau d'autodiagnostic de l'annexe 1 vous a permis d'identifier, lors de la deuxième étape, que les enjeux de sécurité du système d'information étaient limités et que les besoins de sécurité étaient faibles ;
  - Pour une analyse des risques simplifiée, vous pouvez alors procéder à une analyse des risques de survol.

- Démarche Avancée ou Détaillée
    - Dans le cadre de la mise en œuvre d'une démarche **Avancée** ou **Détaillée**, la mise en œuvre d'une méthode d'analyse des risques éprouvée est très fortement recommandée, telle que la méthode EBIOS;
    - La méthode EBIOS présente les risques et les objectifs de sécurité identifiés dans une **Fiche d'Expression Rationnelle des Objectifs de Sécurité (FEROS) ;**
    - L'analyse est effectuée avec ou sans l'assistance d'un consultant ayant une expérience confirmée de la méthode. Elle nécessite la participation des acteurs clés du téléservice à homologuer, qui sont interrogés sur leurs besoins, leur contexte d'emploi du système et les événements qu'ils redoutent. C'est la direction de l'entreprise ou l'autorité administrative, par exemple, qui fournissent les informations sur les besoins de disponibilité ou de confidentialité du système, ce qui permet d'identifier les objectifs de sécurité du système.

Idéalement, le résultat de l'analyse (la FEROS) peut ensuite constituer un élément du cahier des clauses techniques particulières d'un appel d'offres pour la mise en conformité du téléservice à homologuer. Les soumissionnaires doivent y répondre en indiquant de quelle manière ils proposent d'atteindre les objectifs de sécurité identifiés.

Livrable(s) produit(s) :

- La validation des analyses de risques existantes (rapport et FEROS) est consignée dans le compte rendu de réunion de la commission d'homologation ;
- Sinon les résultats des analyses demandées par la Commission d'homologation.

2. Identifier les mesures de sécurité

À l'issue de l'analyse de risque, il convient de définir les mesures de sécurité permettant de couvrir les risques identifiés. Ceux qui demeurent après l'application des mesures sont considérés comme des *risques résiduels* qui doivent être acceptés dans le cadre de l'homologation.

- Démarche simple
    - Pour déterminer les mécanismes de sécurité à mettre en œuvre, vous pouvez également vous référer à plusieurs documents publiés par l'ANSSI (sur http://www.ssi.gouv.fr) :
        - le guide d'hygiène informatique ;
        - le guide d'externalisation pour les systèmes d'information ;
        - le guide sur la virtualisation ;
        - les notes techniques, notamment celle sur la sécurité web.
- Démarche Avancée ou Détaillée
    - Dans le cadre d'une démarche avancée ou détaillée, les objectifs de sécurité identifiés au cours de l'analyse des risques selon la méthode EBIOS permettront de définir les mesures de sécurité destinées à couvrir les risques considérés comme inacceptables.

Outre les documents présentés dans le paragraphe précédent, de nombreux référentiels de sécurité proposent des catalogues de mesures.

Livrable(s) produit(s) :

- L'analyse de risques produite sera complétée avec les mesures de réduction des risques si l'objectif de sécurité dans le traitement retenu est la réduction des risques ;
- Les mesures de sécurité seront choisies dans différents référentiels, dont les exigences du RGS de Polynésie française ;
- Si le traitement des risques est le transfert du ou des risques, alors il conviendra de justifier du choix et des moyens contractuels mis en œuvre.

Etape 6 : Evaluation et amélioration du niveau de sécurité du téléservice

Durant la sixième étape, vous devez mesurer l'écart entre les résultats de l'étude des risques et la réalité, en réalisant un contrôle de sécurité plus ou moins formalisé du Téléservice. Ce contrôle peut intervenir à tout moment du cycle de vie du téléservice : en amont, avant la mise en service voir au cours de la conception, mais également en aval, si le Téléservice est déjà opérationnel.

Le degré de formalisation du contrôle dépend de la démarche entreprise. Vous avez déterminé lors de la seconde étape quel type d'audit était adapté. Certains systèmes n'appellent qu'une vérification peu formelle. En revanche, un audit complet et indépendant se justifie dans le cas de systèmes à fort enjeu de sécurité.

Document(s) attendu(s) :

- Analyse d'écart ;
- Audits ;

Participants potentiels à l'Étape 6 :

- Responsables métiers ;
- Assistance à maîtrise d'ouvrage ;
- Experts techniques internes ;
- RSSI ;

1. Réalisation du contrôle de sécurité

- Démarche Simple
  - Pour la démarche Simple, un audit technique est optionnel.

- Démarche Avancée ou Détaillée
  - Pour la démarche **Avancée ou Détaillée**, il est fortement recommandé d'effectuer un audit technique du téléservice. Cet audit permettra de mettre en évidence d'éventuelles failles et d'identifier rapidement les risques encourus par l'organisme.

Les audits doivent être menés dans les formes prévues par le référentiel d'exigences relatif aux prestataires d'audit de la sécurité des systèmes d'information, disponible en ligne sur le site internet www.lexpol.pf

2. Définition du périmètre du contrôle de sécurité

Le contrôle de sécurité effectué, qui peut prendre la forme d'un audit formalisé, porte sur un téléservice dont le périmètre doit être soigneusement délimité par l'autorité d'homologation. Les contrôles peuvent être de différente nature

- Audit de tout ou partie du code source ;
- Audit de la configuration des équipements et des logiciels du Téléservice;
- Audit de l'architecture du système ;
- Audit de l'organisation mise en place, etc..

Pour les Téléservices qui par définition sont ouverts sur le réseau Internet, un test d'intrusions devra être effectué.

3. Conséquences du contrôle sur le dossier d'homologation

Le contrôle de sécurité doit faire l'objet d'une trace écrite. A fortiori, s'il s'agit d'un audit de sécurité, celui-ci doit faire l'objet d'un rapport, qui doit faire apparaître :

- une évolution des menaces sur le téléservice ;
- la découverte éventuelle de nouvelles vulnérabilités ;
- la préconisation de mesures correctrices, le cas échéant.

Le ou les rapports d'audit est ou sont intégré(s) au dossier d'homologation, qui doit être complété en tenant compte des nouveaux risques mis en lumière.

Livrable(s) produit(s) :

- Le rapport d'audit doit faire apparaître clairement les écarts, éventuels, avec l'analyse de risques de l'Étape 5 ;
- L'auditeur doit proposer un ensemble de recommandations dans son rapport afin d'assister la Commission d'homologation dans ses décisions.

Etape 7 : Mesures de sécurité complémentaires pour couvrir les derniers risques

Durant la septième étape, vous devez définir un plan d'action pour amener le risque identifié à un niveau acceptable.

Document(s) attendu(s) :

- L'équipe projet doit proposer ici dans un livrable les options retenues suite à l'audit et aux résultats de ce dernier.

Participants potentiels à l'Étape 7 :

- Responsables métiers ;
- Assistance à maîtrise d'ouvrage ;
- Experts techniques internes ;
- RSSI ;

1. Le traitement du risque

Au vu des résultats de l'analyse de risques (Étape 5) et du contrôle de sécurité (Étape 6), l'autorité d'homologation se prononce sur l'ensemble des risques qui ne sont pas, à ce stade, complètement couverts par des mesures de sécurité. Il convient ainsi, pour tout ou partie de chaque risque de choisir parmi les options suivantes :

- l'**éviter** : changer le contexte de telle sorte qu'on n'y soit plus exposé ;
- le **réduire** : prendre des mesures de sécurité pour diminuer l'impact et/ou la vraisemblance ;
- l'**assumer** : en supporter les conséquences éventuelles sans prendre de mesure de sécurité supplémentaire ;
- le **transférer** : partager les pertes occasionnées par un sinistre ou faire assumer la responsabilité à un tiers.

On peut choisir plusieurs options pour chaque risque. Par exemple, un risque peut être partiellement réduit par la mise en œuvre de mesures de sécurité, partiellement transféré par le recours à une assurance et partiellement assumé pour ce qui subsiste.

2. La mise en œuvre de mesures de sécurité

Les mesures de sécurité peuvent être de nature technique, organisationnelle ou juridique. Elles sont décidées par l'autorité d'homologation sur proposition de la commission d'homologation.

En cas de recours à un prestataire externe (hébergement de site ou de services par exemple), les mesures de sécurité peuvent être intégralement mises en œuvre à travers un contrat garantissant, par exemple, que les processus et les données sont protégés et accessibles uniquement aux utilisateurs légitimes. Dans ce cas, le responsable du Téléservices s'assurera de la juste prise en compte des risques identifiés lors de

l'Étape 5 en les formalisant dans un Plans d'Assurance Sécurité sur lequel s'engagera le Prestataire d'hébergement ou de service.

3. Définition du plan d'action

Les risques résiduels identifiés lors du contrôle et de l'analyse de risques et qui ne peuvent pas être couverts par des mesures techniques ou organisationnelles sont identifiés dans un plan d'action. Ce dernier indique les vulnérabilités éventuelles, leur degré (critique, majeure, mineure…), l'action correctrice envisagée, le pilote désigné, ainsi que l'échéance associée.

Livrable(s) produit(s) :

- Un rapport formalisant les mesures de sécurité retenues par l'équipe projet en conformité avec les rapports d'audit.

Etape 8 : Décision d'homologation du téléservice

Durant la huitième étape, vous devez concrétiser la décision d'homologation par une attestation formelle autorisant, du point de vue de la sécurité, l'exploitation du téléservice.

La décision d'homologation est l'acte par lequel le responsable de l'autorité administrative atteste de l'existence d'une analyse de sécurité et de sa prise en compte. La décision d'homologation doit nécessairement comprendre un certain nombre d'éléments, référencés ci-dessous.

Document(s) attendu(s) :

- Dossier d'homologation

Participants à l'Étape 8 :

- Commission d'homologation
- Autorité d'homologation

1. Le périmètre de l'homologation

Il doit, au minimum, tenir compte des éléments suivants :

- référentiel réglementaire (dans le cas des téléservices mis en œuvre par les autorités administratives, il s'agit du Référentiel Général de Sécurité de la Polynésie française) ;
- références des pièces du dossier d'homologation ;
- périmètre géographique et physique (localisations géographiques, locaux, etc.) ;
- périmètre fonctionnel et organisationnel (fonctionnalités, types d'informations traitées par le téléservice et sensibilité, types d'utilisateurs, règles d'emploi, procédures, conditions d'emploi des produits de sécurité, etc.) ;
- périmètre technique (cartographie, architecture détaillée du téléservice, produits agréés, prestataires qualifiés, etc.).

2. Les conditions accompagnant l'homologation

L'autorité d'homologation peut, en fonction des risques résiduels identifiés, assortir l'homologation de conditions d'exploitation ainsi que d'un plan d'action visant à maintenir et à améliorer le niveau de sécurité du téléservice dans le temps. À chaque action, ce plan associe une personne pilote ainsi qu'une échéance.

3. La durée de l'homologation

L'homologation doit être décidée pour une durée maximale.

Cette durée doit prendre en compte l'exposition du système d'information aux nouvelles menaces, ainsi que les enjeux de sécurité du téléservice, c'est-à-dire le degré de criticité des informations et des processus du système.

Pour un téléservice bien maîtrisé, avec peu de risques résiduels et ne présentant pas de difficultés particulières, il est recommandé de prononcer une homologation d'une durée maximale de cinq (5) ans,

avec revue annuelle. Cette durée maximale doit être réduite à trois (3) ans pour un système avec de quelques risques résiduels ou à un an (1) pour un système présentant de nombreux risques résiduels.

4. Conditions de suspension ou de retrait de l'homologation

L'homologation de sécurité ne demeure valide que tant que le système d'information est exploité dans le contexte décrit dans le dossier d'homologation. Les changements suivants doivent impliquer un réexamen du dossier, pouvant conduire à une nouvelle décision d'homologation ou à un retrait de la décision :

- raccordement d'un nouveau site sur le téléservice ;
- ajout d'une fonctionnalité majeure ;
- succession de modifications mineures ;
- réduction de l'effectif affecté à une tâche impactant la sécurité ;
- changement d'un ou de plusieurs prestataires ;
- prise de fonction d'une nouvelle autorité d'homologation ;
- non-respect d'au moins une des conditions de l'homologation ;
- changement du niveau de sensibilité des informations traitées et, plus généralement, du niveau du risque ;
- évolution du statut de l'homologation des systèmes interconnectés ;
- publication d'incidents de nature à remettre en cause les garanties recueillies dans le dossier de sécurité ;
- décision de l'autorité d'homologation.

À ce titre, il est recommandé que la commission d'homologation soit réunie annuellement par l'autorité d'homologation, afin de procéder à une revue du respect des conditions de l'homologation.

Livrable(s) produit(s) :

- Décision d'homologation

Etape 9 : Surveillance des risques résiduels du téléservice

Durant cette dernière étape, qui intervient après la décision d'homologation proprement dite, vous devez mettre en œuvre une procédure de révision périodique de l'homologation, ainsi que le plan d'action pour traiter les risques résiduels et les nouveaux risques dans le cycle de vie du téléservice.

Document(s) attendu(s) :

- Dossier d'homologation
- Nouveaux audits
- Evolutions
- Incidents

Participants à l'Étape 9 :

- Commission d'homologation

1. Suivi de l'homologation

À la suite de la décision proprement dite, l'autorité d'homologation doit veiller au maintien du niveau de sécurité du téléservice. La commission d'homologation réalise annuellement un suivi de l'homologation. Cette étape n'est pas une nouvelle instruction. Elle doit donc rester simple et se limiter à une mise à jour du dossier et à une analyse succincte des évolutions et des incidents intervenus au cours de l'année, afin de juger de l'opportunité d'une révision plus approfondie de l'homologation.

En préparation du renouvellement de l'homologation, le dossier d'homologation est régulièrement complété par les éventuelles analyses de vulnérabilités, les comptes rendus de contrôle et les rapports d'audits complémentaires. La version consolidée est transmise aux membres de la commission d'homologation

Il est recommandé de réunir périodiquement la commission d'homologation pour reprendre la liste des critères et vérifier que les conditions d'homologation sont toujours respectées. Cela permet également d'éviter de reprendre l'homologation à zéro au terme de sa durée de validité.

2. Maintien en conditions de sécurité

Il est nécessaire que les conditions de l'homologation soient respectées dans le temps. À ce titre, l'entité en charge du maintien du dossier d'homologation doit également assurer une veille technologique. Celle-ci permet d'identifier les vulnérabilités qui apparaîtraient sur le téléservice et s'assurer qu'elles soient corrigées, notamment les plus sérieuses.

Il est également nécessaire de vérifier :

- les clauses de sécurité et de maintien en conditions de sécurité du téléservice, le cas échéant en se référant au guide d'externalisation publié par l'ANSSI ;
- les capacités d'évolution et d'interopérabilité de son système, notamment au regard de ses capacités de développement ou de ses contrats de prestations de service.

Livrable(s) produit(s) :

- Dossier d'homologation mis à jour

CONSEILS PRATIQUES

La démarche d'homologation est un projet en soi, qui doit s'intégrer complètement au projet global et au cycle de vie du système d'information, le téléservice. C'est une démarche qui peut se révéler complexe et qui se heurte parfois à des difficultés organisationnelles, techniques ou calendaires. Les conseils contenus dans cette fiche vous permettront d'aboutir plus facilement à un résultat satisfaisant.

1. Conseils d'ordre général

Les conseils d'ordre général listés ci-dessous doivent, dans la mesure du possible, être suivis pour maximiser les chances de réussite d'une démarche d'homologation :

- débuter suffisamment tôt la démarche d'homologation ;
- prévoir une validation formelle des décisions au niveau hiérarchique adéquat ;
- désigner un véritable chef de projet, qui sera disponible tout au long du projet ;
- maîtriser le calendrier et ne pas être trop contraint par des nécessités opérationnelles ;
- bien définir le périmètre et disposer d'une architecture précise du système ;
- bien prendre en compte les interconnexions éventuelles ;
- s'appuyer sur des documents écrits, explicites, sans ambiguïté, afin d'éviter les quiproquos entre les parties prenantes au projet.

2. Avant l'étude

Une réflexion menée en amont permet de bien préparer la démarche d'homologation et d'assurer sa réussite de façon optimale.

Au préalable, il faut que la démarche soit portée à haut niveau par l'autorité d'homologation et que l'ensemble des acteurs concernés soit impliqué et motivée.

Il faut également désigner un chef de projet, qui disposera des moyens pour mener à bien sa mission et rapporter toute difficulté à l'autorité d'homologation.

Enfin, dès que les acteurs de l'homologation sont identifiés, il est indispensable de les sensibiliser sur la démarche, les concepts et le vocabulaire qui seront utilisés.

3. Pendant l'étude

Pour chaque activité à réaliser, il est conseillé de s'organiser en mode projet, en identifiant un responsable de l'activité, en constituant un groupe de travail et en lui confiant une mission précise, associée à une date de réalisation.

Certaines missions sont essentielles pour la réussite du projet :

- la sensibilisation des acteurs
    - rappeler l'objectif de l'activité
    - présenter les concepts, le vocabulaire
    - s'assurer que l'ensemble des acteurs ait une vision commune de la problématique
- la collecte des informations
    - réaliser des entretiens
    - rassembler les documents existants sur l'organisme, le projet de téléservice
- le suivi du projet
    - présenter des exemples pour lancer les discussions
    - synthétiser les informations récoltées pour validation par le groupe de travail
    - nommer des responsables et fixer des échéances
    - se rencontrer périodiquement

Il est également nécessaire d'adapter les livrables aux destinataires en ce qui concerne :

- la forme : tableaux, textes, schémas, etc. ;
    - le niveau d'information : recherche d'exhaustivité ou forme synthétique ;
    - l'intégration aux documents existants ;
    - l'adaptation au vocabulaire habituel de l'organisme,
    - leur nomenclature, qui doit être explicite,
    - leur libellé, qui doit être court et descriptif.

Enfin, il est recommandé de faire valider chaque étape par la commission d'homologation. Cela permet d'éviter les retours en arrière improductifs, tout en impliquant les autorités tout au long de la réalisation du dossier de sécurité.