DTSI/Dir DTSI
CB

Extrait du Registre des Délibérations

réunion : Juin 2014

séance du 27/06/14

N° : A9

Politique qualité et performance de l'administration

Objet : Homologation de télé-services mis en oeuvre au sein du Conseil Général du Var.

Le Conseil Général s'est réuni à Toulon à 09h30, sous la Présidence de Monsieur Horace LANFRANCHI, Président du Conseil Général du Var.

Le Conseil Général est appelé à examiner l'affaire citée en objet et qui est inscrite au bordereau des rapports de Monsieur le Président.

.

Présents : Monsieur Jean-Louis ALENA, Madame Véronique BACCINO, Monsieur Ferdinand BERNHARD, Monsieur Jean BOMBIN, Monsieur Michel BONNUS, Madame Raymonde CARLETTI, Monsieur Pierre-Yves COLLOMBAT, Madame Caroline DEPALLENS, Monsieur Jean-Guy DI GIORGIO, Madame Françoise DUMONT, Madame Nicole FANELLI, Monsieur Marc GIRAUD, Monsieur André GUIOL, Monsieur Pierre LAMBERT, Monsieur Horace LANFRANCHI, Monsieur Guy LOMBARD, Monsieur Laurent LOPEZ, Monsieur Barthélemy MARIANI, Monsieur Jean-Louis MASSON, Monsieur Guy MENUT, Monsieur Joseph MULE, Monsieur Michel PARTAGE, Monsieur Claude PIANETTI, Monsieur Max PISELLI, Monsieur Jacques POLITI, Madame Josette PONS, Monsieur Louis REYNIER, Monsieur Bernard ROLLAND, Monsieur Francis ROUX, Monsieur Philippe SANS, Monsieur Jean-Pierre SERRA, Monsieur Alain SPADA, Monsieur Albert VATINET, Monsieur Gilles VINCENT, Monsieur Philippe VITEL.

Procurations : Madame Hélène AUDIBERT à Madame Josette PONS, Monsieur Elie BRUN à Monsieur Bernard ROLLAND, Monsieur François CAVALLIER à Monsieur Max PISELLI, Monsieur Robert CAVANNA à Monsieur Marc GIRAUD, Monsieur Paul DENIS à Monsieur Jean-Pierre SERRA, Monsieur Patrick MARTINENQ à Monsieur Pierre-Yves COLLOMBAT, Monsieur Ange MUSSO à Monsieur Joseph MULE.

Excusés : .

Absents : Monsieur Jean-François FOGACCI.

Au nom de la Commission Finances et Patrimoine, Monsieur Jean-Pierre SERRA, rapporteur, expose :

En application de l'ordonnance dite « télé-services » du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, il vous est proposé l'homologation de sept télé-services mis en œuvre au sein de la collectivité.

Par télé-services, il faut entendre, tous les échanges électroniques entre les administrations et les usagers ainsi que les échanges électroniques entre les administrations elles-mêmes : courrier électronique, transferts de données via une application, échanges d'information sur un site internet.

L'homologation est formalisée par un document qui atteste de la conformité d'une application ou d'un télé-service aux règles définies par le Référentiel général de sécurité (RGS) établi par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Le référentiel général de sécurité fixe les règles auxquelles les systèmes d'information mis en place par les autorités administratives doivent se conformer pour assurer la sécurité des informations échangées, et notamment leur confidentialité et leur intégrité, ainsi que la disponibilité et l'intégrité de ces systèmes et l'identification de leurs utilisateurs.

Le document d'homologation est établi par une commission d'homologation dédiée, interne à la collectivité. Il comprend, pour chaque télé-service :

- une analyse des risques en matière de sécurité des systèmes et données,
- une définition des travaux à réaliser pour réduire ces risques, si nécessaire,
- la planification des travaux de mise en sécurité,
- une proposition d'homologation pour une durée déterminée, ou un refus d'homologation ou une homologation temporaire jusqu'à la réalisation des travaux nécessaires.

*
* *

Le Conseil Général,

VU le code général des collectivités territoriales,

VU 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, et le décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9 à 12 de l'ordonnance,

VU le décret n° 2007-284 du 2 mars 2007 fixant les modalités d'élaboration, d'approbation, de modification et de publication du référentiel général d'interopérabilité,

VU l'arrêté du 9 novembre 2009 portant approbation du référentiel général d'interopérabilité,

VU l'arrêté du 6 mai 2010 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques,

VU le référentiel général d'interopérabilité, version 1.0 du 12 mai 2009, de la Direction générale de la modernisation de l'Etat du ministère du Budget, des Comptes publics et de la Fonction publique,

VU le référentiel général de sécurité, version 1.0 du 6 mai 2010 de l'Agence nationale de sécurité des systèmes d'information et de la Direction générale de la modernisation de l'Etat du ministère du Budget, des Comptes publics et de la Fonction publique,

CONSIDERANT que constitue un télé-service, tout système d'information permettant aux usagers ou autorités administratives de procéder, par voie électronique, à des démarches ou formalités administratives,

CONSIDERANT que le Conseil général du Var doit, en application de la réglementation en vigueur, homologuer les sept télé-services qu'il a créés et actuellement en service,

CONSIDERANT que l'homologation doit intervenir selon le protocole, joint en annexe à la présente délibération,

CONSIDERANT qu'une commission d'homologation, créée à cet effet, a examiné les dossiers constitués en vue de l'homologation de ses télé-services,

CONSIDERANT que ces télé-services peuvent être homologués dans les conditions suivantes :

Nom du télé-service	Homologation	Réserve
1 - Plate-forme Marchés publics A.W.S	3 ans	Sans objet
2 – Site des Archives Départementales	3 ans	Sans objet
3 – Site Var.fr	3 ans	Sans objet
4 – Prestataires sociaux	1 an	Fourniture par le prestataire des informations sur ses pratiques de sécurité
5 – Billettique Transports	3ans	Sans objet
6 – Site de la Médiathèque	1 an	Mise en place d'un protocole sécurisé (http)
7- Télétransmission des actes	3 ans	Sans objet

CONSIDERANT qu'il convient de déléguer à la Commission Permanente du Conseil Général les futures décisions à prendre pour tous nouveaux télé-services que le Département créera, ainsi que pour toute homologation,

Après en avoir délibéré,

DECIDE

- de prononcer, par la présente délibération, l'homologation des sept télé-services décrits dans le tableau ci-dessus, conforme aux prescriptions et aux mesures du protocole d'homologation, pour la durée et sous les réserves mentionnées,

- de déléguer à la Commission Permanente toutes décisions à prendre en matière de création et d'homologation de télé-services.

Adopté à l'unanimité.

Signé : Horace LANFRANCHI
Président du Conseil Général du Var

Réception au contrôle de légalité : 04/07/14

Référence technique : 093-228300018-20140627-lmc117647-DE-1-1

Acte certifié exécutoire
le 08/07/2014

Pour le Président du Conseil Général,
le Directeur Général des Services,
Alain PRUVOST

Annexe N° à la Délibération N° du

Homologation Référentiel Général de Sécurité

Protocole d'homologation d'un télé-service

CG83

Table des matières

1. INTRODUCTION

1.1. Objet du document

Ce document décrit le protocole d'homologation d'un téléservice conformément au Référentiel Général de Sécurité prévu par l'article 9 de l'ordonnance n°2005-1516 du 8 décembre 2005 et son décret d'application n°2010-11 2 du 2 février 2010.

1.2. Règlementation

Le référentiel général de sécurité (RGS), prévu par l'article 9 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, et approuvé par l'arrêté du 6 mai 2010, a été élaboré conjointement par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et par la Direction générale de la modernisation de l'État (devenue la Direction interministérielle pour la modernisation de l'action publique).

Le référentiel général de sécurité fixe les règles auxquelles les systèmes d'information mis en place par les autorités administratives doivent se conformer pour assurer la sécurité des informations échangées, et notamment leur confidentialité et leur intégrité, ainsi que la disponibilité et l'intégrité de ces systèmes et l'identification de leurs utilisateurs.

L'ordonnance n°2005-1516 renvoie à des décrets les conditions d'application des mesures qu'elle prévoit. En particulier, le décret n°2010-1 12 du 2 février 2010 et son article 5:

L'autorité administrative atteste formellement auprès des utilisateurs de son système d'information que celui-ci est protégé conformément aux objectifs de sécurité fixés en application de l'article 3.

Dans le cas d'un téléservice, cette attestation est rendue accessible aux usagers selon les mêmes modalités que celles prévues à l'article 4 de l'ordonnance du 8 décembre 2005 susvisée pour la décision de création du téléservice.»

Cette « attestation formelle », évoquée à l'article 5 du décret n°2010-112, correspond à une « homologation de sécurité du système d'information ». Celle-ci est obligatoire et est un préalable à la mise en service opérationnelle de tout système d'information. Elle est prononcée par une autorité dite d'homologation.

1.3. Délai de mise en conformité

Télé-services existants - Conformément à l'article 14 de l'ordonnance n°2005-1516 du 8 décembre 2005, la conformité de chaque téléservice existant doit être assurée avant le 18 mai 2013.

Nouveaux télé-services - La conformité de tout nouveau téléservice devra être assurée avant sa mise en service opérationnel.

1.4. L'homologation

1.4.1. Décision d'homologation

La décision d'homologation, ou « attestation formelle », est l'engagement par lequel l'autorité d'homologation (constituée au sein de l'autorité administrative) atteste que le projet (ici téléservice) 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.

Afin que sa décision soit motivée et justifiée, il est recommandé que l'autorité d'homologation s'appuie sur un dossier de sécurité. Ce dossier est constitué sur la base d'une analyse de risques du système d'information matérialisant le téléservice.

Au sein du conseil général du var, la décision d'homologation sera matérialisée par une délibération soumise au vote de l'Assemblée.

1.4.2. Commission d'homologation

La mise en œuvre du R.G.S n'étant pas uniquement une question technique, mais véritablement une politique globale de sécurité, la Commission d'homologation est constituée :

- d'une M.O.A comprenant : Le Président du CG83 (Autorité Administrative), le D.G.S, les Délégués Généraux,
- d'une M.O.E comprenant : La D.T.S.I, la Direction des Affaires Juridiques, des prestataires juridiques ou techniques

1.4.3. Décision d'homologation

Selon les résultats de l'analyse effectuée lors de la démarche d'homologation, la Commission d'homologation pourra prononcer :

- Une homologation provisoire, assortie de réserves et d'un délai de mise en conformité des défauts de sécurité rencontrés ;
- Une homologation, assortie le cas échéant de conditions, pour une durée de 3 ans ;
- Un refus d'homologation, si les résultats de l'audit font apparaître des risques résiduels jugés inacceptables.

1.4.4. Publication de l'homologation

La décision d'homologation devant être rendue accessible aux utilisateurs du téléservice, elle fait l'objet d'une publicité sur le support correspondant au téléservice (application, internet...).

1.5. Dossier de sécurité du téléservice

De façon à ce que la décision d'homologation soit motivée et justifiée, l'autorité d'homologation s'appuie sur un dossier de sécurité.

Le dossier de sécurité est composé des documents suivants :

- La synthèse du dossier (présent document),
- Rapport d'analyse de risques du téléservice,
- Plan d'actions complémentaires visant à réduire encore les risques identifiés,
- Fiches de suivi des actions.

2. METHODE D'ANALYSE UTILISEE

Conformément aux exigences du RGS et aux différentes préconisations énoncées dans les guides associés, la méthode retenue visant à identifier, apprécier et traiter les risques relatifs aux systèmes d'information pesant sur le téléservice est la méthode EBIOS 2010.

La méthode EBIOS permet l'analyse des risques selon les étapes suivantes :

- 1 - Etude du contexte,
- 2 - Etude des évènements redoutés,
- 3 - Etude des scénarios de menaces,
- 4 - Etude des risques,
- 5 - Etude des mesures de sécurité (actuellement mise en œuvre et mesures inscrites au plan d'actions).

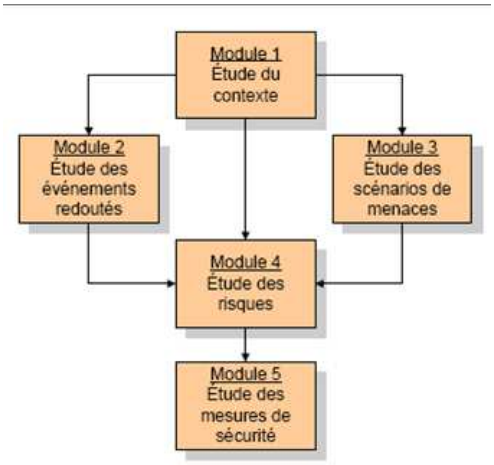


Figure 1 : Démarche EBIOS globale

Comme illustré sur la figure 1, l'analyse de risques est composée de cinq étapes.

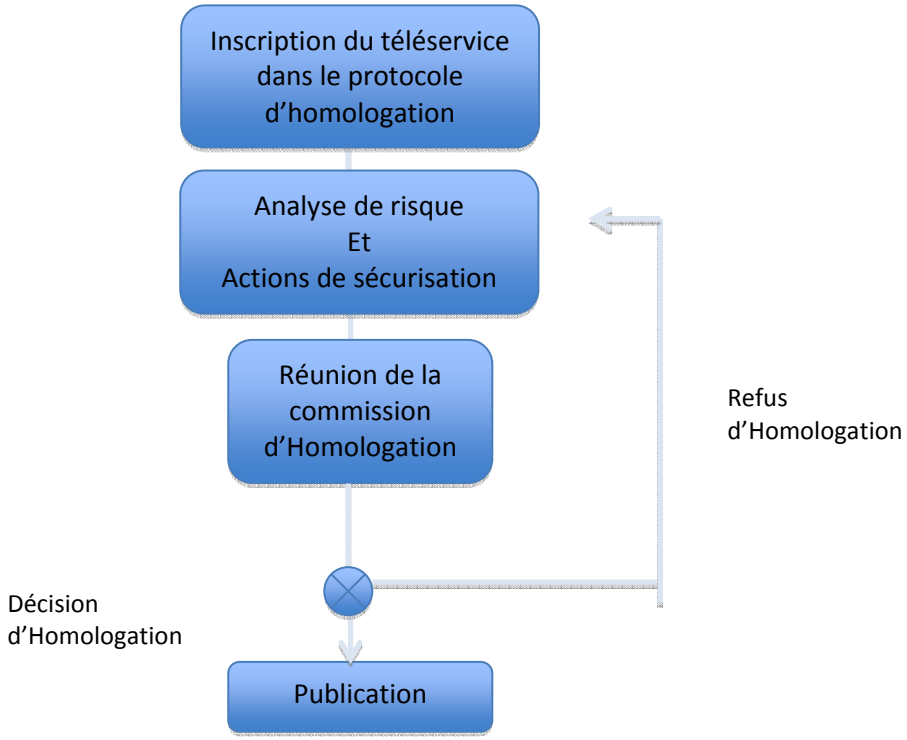
L'étude du contexte permet de cadrer l'analyse et d'acquérir une bonne connaissance du téléservice, de ses contraintes et enjeux métier. Les étapes suivantes sont l'étude des évènements redoutés, qui permet d'identifier les biens essentiels et leur criticité, et l'étude des scénarios de menaces qui recense les vulnérabilités pesant sur la cible de l'étude.

La confrontation des scénarios de menaces aux évènements redoutés permet ensuite de retenir et hiérarchiser les risques susceptibles de porter atteinte aux biens essentiels du téléservice.

La stratégie de gestion des risques consiste ensuite à identifier les risques acceptables tenant compte des mesures de sécurité existantes et les risques pour lesquels des mesures de sécurité complémentaires doivent être mises en place.

L'étape de détermination des mesures de sécurité complémentaire spécifie les mesures techniques, procédurales et organisationnelles de sécurité devant être mises en place pour répondre aux risques identifiés, et ainsi diminuer la probabilité d'occurrence, ou limiter l'impact des risques qu'il convient de traiter. Les risques résultant de cette étape sont dits résiduels. Ces risques et niveaux associés font l'objet d'une acceptation formelle dans le cadre de l'homologation.

3. PROTOCOLE D'HOMOLOGATION



3.1. Inscription du téléservice dans le protocole d'homologation

L'homologation est obligatoire et est un préalable à la mise en service opérationnelle de tout système d'information.

Dans cette première phase de mise en conformité, la DTSI du Conseil Général a inscrit au protocole d'homologation 7 télé-services identifiés comme sensibles :

- Site Var.fr
- Archives Départementales
- Médiathèque

- Prestataires sociaux
- AWS - Plate-forme "Marchés Publics »
- Billettique transport
- Télétransmission d'actes en préfecture

Par la suite, chaque nouveau téléservice sera inscrit automatiquement dans le protocole d'homologation.

3.2. Analyse de risques et actions de sécurisation

Ce chapitre présente la démarche d'analyse de risques pour un téléservice. Celle-ci sera déployée pour chaque téléservice devant faire l'objet d'une homologation.

Cette phase résulte sur la consolidation de dossier de sécurité, document support au protocole d'homologation permettant de motiver et justifier la décision d'homologation.

3.2.1. Etape n°1 : étude du contexte

Objectifs

- Définir le cadre de l'analyse et en formaliser le périmètre

Actions

- Formalisation des métriques d'analyse de risque
- Appropriation de l'architecture fonctionnelle et technique du téléservice
- Définition du niveau de granularité à adopter pour l'analyse
- Recensement des biens essentiels et des biens supports (vue globale, vue par élément de la cible, vue par entité du réseau)
- Identification des parties prenantes et paramètres à prendre en compte (contraintes)

Résultats

- Document Annexes de métrique
- Identification des parties prenantes
- Recensement des biens essentiels et supports
- Saisie du volet « étude du contexte » dans l'outil EGERIE Risk Manager pour l'analyse

Modalités pratiques

- L'appropriation de l'architecture fonctionnelle et technique est effectuée sur une base documentaire, confortée lors d'entretiens avec l'équipe de la DTSI concernée par le téléservice.

- Les échelles de métriques (besoins, événements redoutés, vulnérabilités et risques) ont été définies (Cf. Document Annexe de métriques).
- La cartographie des biens essentiels et des biens supports est réalisée au moyen de la revue documentaire, et des entretiens avec les intervenants de la DTSI concernés. Les biens essentiels sont associés aux actifs du réseau, ainsi qu'aux biens supports. Une cartographie globale est alors établie avec les associations biens essentiels / biens supports.
- Les différentes parties prenantes prenant part au téléservice sont aussi identifiées : services et intervenants de la DTSI, directions métiers, sous-traitants, fournisseurs… Ces parties prenantes seront sollicitées durant les étapes suivantes sous la forme d'entretiens individuels ou par réponse à des questionnaires.
- Les entretiens sont effectués avec :
  - Les membres de la DTSI en charge des actifs du téléservice (enjeux, besoins, biens essentiels, métriques, biens supports dans une certaine mesure, granularité de l'étude),
  - D'autres intervenants identifiés en collaboration avec le responsable du téléservice au lancement ou durant l'analyse.

3.2.2. Etape n°2 : étude des événements redoutés

Objectifs

- Recenser et caractériser les événements redoutés
- Identifier les besoins de sécurité de chaque élément essentiel

Actions

- Identifier les éléments redoutés en collaboration avec les responsables du téléservice
- Caractériser la sensibilité (DICP) des biens essentiels
- Formaliser les scénarios d'événements redoutés et en caractériser les conséquences
- Hiérarchiser les événements redoutés

Résultats

- Evénements redoutés recensés et caractérisés
- Besoins de sécurité recensés par bien essentiel
- Saisie du volet « événements redoutés » et estimation des conséquences DICP pour chaque bien essentiel dans le logiciel EGERIE RISK MANAGER.

Modalités pratiques

- L'identification des événements redoutés, et leur caractérisation sont effectuées en collaboration avec la MOA de la DTSI et éventuellement les acteurs métier du téléservice.
- L'identification des besoins de sécurité de chaque élément essentiel est également effectuée en collaboration avec ces mêmes acteurs. (identification des

applications et données critiques en matière de disponibilité, et sur les autres critères retenus pour l'analyse).

- La formalisation des scénarios et leur hiérarchisation sont effectuées sur la base des informations recueillies.

3.2.3. Etape n°3 : étude des scénarios de menaces

Objectifs

- Identifier les vulnérabilités techniques
- Analyser les scénarios de menaces
- Analyser les mesures existantes
- Evaluer la vraisemblance des scénarii et les hiérarchiser

Actions

- Etude des menaces et de leurs sources
- Etude des vulnérabilités et des mesures de sécurité existantes
- Formalisation des scénarios et analyse de leur vraisemblance

Résultats

- Scénarios de menaces formalisés, caractérisés et hiérarchisés
- Vulnérabilités techniques initiales identifiées
- Mesures de sécurité existantes renseignées
- Etude des besoins en prestataires de service qualifié au sens RGS
- Etude des besoins en produits certifiés
- Saisie des scénarios de menaces et caractérisation dans le logiciel EGERIE Risk Manager, pour l'analyse (prise en compte des vulnérabilités spécifiques)
- Saisie des résultats de l'analyse dans le module « Mesures existantes » du logiciel
- Dossier de sécurité (version 0.1) DS_v0.1

Modalités pratiques

- L'analyse des menaces et l'identification des vulnérabilités sont effectuées en collaboration avec les équipes de la DTSI et éventuellement des métiers.
- L'identification des mesures de sécurité est réalisée sur la base d'entretiens ou de questionnaires émis aux différentes parties prenantes : DTSI, Prestataires et fournisseurs impliqués dans le téléservice.
- Cette étape permet aussi d'identifier la nécessité d'utiliser ou non des prestataires de service qualifiés ou des produits certifiés afin d'assurer la sécurité de certaines fonctions sensibles spécifiées dans le RGS (Signature électronique et horodatage par exemple).
- Cette étape est finalisée par une réunion de travail avec les intervenants impliqués (DTSI et métier), afin de valider les événements, les menaces et vulnérabilités identifiées, et leur vraisemblance.

3.2.4. Etape n°4 : étude des risques

Objectifs

- Définir une cartographie des risques

Actions

- Confronter les scénarios de menaces aux événements redoutés
- Formaliser les risques et les hiérarchiser
- Valider les scénarios en réunion de travail

Résultats

- Cartographie des risques
- Saisie des scénarios de risques dans le logiciel EGERIE Risk Manager
- Dossier de sécurité (version 0.2) DS_v0.2

Modalités pratiques

- Les scénarios de menaces sont confrontés aux événements redoutés; des scénarios de risques sont proposés, illustrant les principaux risques, hiérarchisés en fonction de leur vraisemblance et de leur gravité
- Une cartographie des risques pour le téléservice est proposée. Cette cartographie présente les risques actuellement présents sur le téléservice en tenant compte des mesures de sécurité existantes.
- Une réunion avec le chef de projet est dévolue à la validation des différents scénarios proposés

3.2.5. Etape n°5 : étude des mesures de sécurité co mplémentaires

Objectifs

- Identifier les mesures de sécurité complémentaires au traitement de chaque scénario de risque retenu parmi la liste à traiter
- Définir le plan d'action proportionné aux risques
- Définir des principes et des moyens de supervision pour les risques non couverts
- Suivre les actions de traitement

Actions

- Sélectionner les mesures de sécurité complémentaires au sein de chaque risque à traiter
- Réaliser les associations scénarios de risques / mesures dans le logiciel EGERIE RISK MANAGER
- Recenser les risques non couverts et définir les procédures et moyens de suivi
- Consolider les résultats avant la réunion de la commission d'homologation

Résultats

- Mesures de sécurité complémentaires, spécifiées pour la réduction des risques. Ces mesures sont inscrites au plan d'action.
- Liens établis et outillés entre scénarios de risques et mesures
- Risques non couverts listés ; procédures et moyens de suivi spécifiés
- Suivi des actions
- Dossier de sécurité (version 1.0) DS_v1.0

Modalités pratiques

- Des mesures de sécurité complémentaires sont définies visant à réduire les risques résiduels à un niveau acceptable.
- Les mesures sont renseignées dans le logiciel, avec les éléments de liaison les associant aux scénarios de risques, et caractérisées par un indicateur de couverture permettant d'avoir une réévaluation du niveau de risque une fois les mesures en place. Il est ainsi possible de disposer d'un aperçu du niveau de risque hors mesure planifiée, et du niveau de risque résiduel à terme lorsque les mesures seront en place.
- Une réunion avec le chef de projet est organisée pour présenter les résultats de l'analyse de risque.
- Le plan d'actions est défini et suivi par un expert.
- Le dossier de sécurité du téléservice est alors consolidé. Il contient le rapport d'analyse de risques, le plan d'actions de traitement des risques et les fiches de suivi de traitement.

3.3. Réunion de la commission d'homologation

La commission d'homologation doit être réunie. La direction de la DTSI programme avec les membres de la commission d'homologation les différentes dates de réunions.

3.4. Publication de la décision

Une fois la décision d'homologation du téléservice obtenue. Celle-ci doit faire l'objet d'une publicité sur le support correspondant au téléservice (application, internet...).

3.5. Durée de validité

L'homologation d'un téléservice est valable 3 ans.

Durant trois ans, la situation à risque peut évoluer : nouvelles menaces, nouvelles vulnérabilités, modification de l'architecture du téléservice, nouvelles fonctionnalités,...

Ainsi, à la fin de cette période de 3 ans, le téléservice doit, à nouveau, suivre le protocole d'homologation et faire l'objet d'une nouvelle homologation.