DELIBERATION DU CONSEIL MUNICIPAL

SEANCE DU **15 décembre 2021 à 16 h 00**

AUJOURD'HUI **quinze décembre deux mille vingt et un**

LE CONSEIL MUNICIPAL de la Ville de Clermont-Ferrand, convoqué par Monsieur le Maire le 09 décembre 2021, s'est réuni dans les Salons de l'Hôtel de Ville.

Après avoir ouvert la séance, Monsieur le Maire procède à l'appel.

Etaient présents Mmes et MM. les Membres du Conseil dont les noms suivent :

Olivier BIANCHI, Maire, présidant la séance

Présent(e)s : Olivier BIANCHI, Christine DULAC ROUGERIE, Nicolas BONNET, Marion CANALES, Cyril CINEUX, Isabelle LAVEST, Grégory BERNARD, Manuela FERREIRA DE SOUSA, Rémi CHABRILLAT, Nicaise JOSEPH, Jean-Christophe CERVANTES, Cécile AUDET, Jérôme GODARD, Christophe BERTUCAT, Magali GALLAIS, Jérôme AUSLENDER, Anne-Laure STANISLAS, Didier MULLER, Sondès EL HAFIDHI, Charles-André DUBREUIL, Sylviane TARDIEU, Dominique ADENOT, Anna AUBOIS, Marion BARRAUD, Laetitia BEN SADOK, Valérie BERNARD, Fatima BISMIR, Alexis BLONDEAU, Julien BONY, Dominique BRIAT, Fatima CHENNOUF-TERRASSE, Alparslan COSKUN, Samir EL BAKKALI, Eric FAIDY, Christiane JALICON, Claudine KHATCHADOURIAN-TECER, Diego LANDIVAR, Cécile LAPORTE, Steve MAQUAIRE-BEAUSOLEIL, Marianne MAXIMI, Pierre MIQUEL, Lucie MIZOULE, Lucas PEYRE, Frédéric PILAUD, Stanislas RENIÉ, Pierre SABATIER, Vincent SOULIGNAC, Yannick VIGIGNOL, Thomas WEIBEL

Excusé(e)s ayant donné pouvoir : Odile VIGNAL à Anne-Laure STANISLAS, Géraldine BASTIEN à Christiane JALICON, Jean-Pierre BRENAS à Julien BONY, Estelle BRUANT à Marion BARRAUD, Wendy LAFAYE à Anna AUBOIS, Catherine PINET-TALLON à Cécile LAPORTE

Excusé(e)s :

Absent(e)s :

Secrétaire : Alexis BLONDEAU

Rémi CHABRILLAT et Cécile LAPORTE arrivent pendant la présentation du diaporama de la question n°2.
Lucie MIZOULE arrive pendant le débat de la question n°2 (fin du pouvoir donné à Magali GALLAIS).

Rapport N° 24
HOMOLOGATION DE SECURITE DES SYSTEMES D'INFORMATION

CONTEXTE LEGAL

L'essor d'internet, du nomadisme, des smartphones ou encore du « cloud computing » ont modifié les comportements et les usages professionnels et personnels. L'administration a ainsi développé des services numériques aux usagers.

La Ville de Clermont-Ferrand s'est engagée dans cette mutation (télé-services sur internet, applications mobiles et traitement dématérialisés) faisant de son système d'information une ressource stratégique pour la délivrance de services publics.

Face à l'ensemble des exigences de sécurité au sein des administrations, l'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers les autorités administratives, a créé le Référentiel Général de Sécurité (RGS) qui constitue le cadre réglementaire permettant d'assurer la sécurité et d'instaurer la confiance dans les échanges au sein de l'administration et avec les citoyens.

Les conditions d'élaboration, d'approbation, de modification et de publication du RGS sont fixées par le décret n°2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance précitée.

Dans ce cadre, la version 2.0 du RGS a été approuvée par l'arrêté ministériel du 13 juin 2014 et est applicable depuis le 1er juillet 2014.

Les règles formulées dans le RGS s'imposent et sont modulées en fonction du niveau de sécurité retenu par l'autorité administrative dans le cadre de la sécurisation des services en ligne dont elle est responsable. La collectivité doit s'y conformer pour assurer la sécurité des informations échangées, et notamment leur confidentialité et leur intégrité, ainsi que la disponibilité et la fiabilité des systèmes utilisés. Ce référentiel fixe ainsi, selon le niveau de sécurité requis, les règles que doivent respecter certaines fonctions contribuant à la sécurité des informations, parmi lesquelles la signature électronique, l'authentification, la confidentialité ou encore l'horodatage.

En complément, le RGS impose aux autorités administratives d'homologuer leurs systèmes d'information et leurs téléservices (échanges d'informations entre Autorités Administratives ou Autorités Administratives et Usagers).

La décision d'homologation de sécurité, également dénommée « attestation formelle » est prononcée par l'autorité d'homologation, désignée par l'autorité administrative chargée du système d'information.

Cette décision, qui s'appuie sur un dossier d'homologation, atteste, au nom de l'autorité administrative, que le système d'information est protégé conformément aux objectifs de sécurités fixés et que les risques résiduels sont acceptés.

Pour ce faire, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a élaboré un guide méthodologique pour aider les autorités administratives dans leur démarche d'homologation de sécurité.

DESCRIPTION DES COMPOSANTS DE L'HOMOLOGATION RGS

Selon le guide d'homologation RGS de l'ANSSI, les acteurs de l'homologation sont ainsi identifiés :

- L'autorité d'homologation,
- le responsable du processus d'homologation,
- la commission d'homologation,
- et d'autres acteurs susceptibles d'intervenir dans le processus. (missions détaillées en annexe)

- Membres permanents de la commission
- Membres occasionnels de la commission (si besoin)

L'autorité d'homologation :

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

L'autorité d'homologation doit être désignée à un niveau hiérarchique suffisant pour assumer toutes les responsabilités afférentes à cette décision d'homologation.

Le responsable du processus d'homologation :

L'autorité d'homologation désigne un responsable du processus d'homologation qui mènera le projet d'homologation en son nom et réunira la commission d'homologation au besoin.

Au regard du niveau de sécurité requis pour le système d'information concerné et/ou d'un besoin spécifique identifié, il pourra décider de consulter des membres occasionnels.

Pour ce faire, le Responsable de Sécurité des Systèmes d'Information (RSSI) est désigné pour mener le projet d'homologation impactant des éléments de sécurités numériques globaux à la collectivité.

La commission d'homologation :

La commission d'homologation assiste l'autorité d'homologation pour instruire 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 système et proportionnées à ses enjeux. Cette commission réunit les responsables métier concernés par le service numérique à homologuer et des experts techniques. Elle peut donc être de taille réduite dans les cas simples.

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.

Le dossier d'homologation :

Le dossier d'homologation est une analyse du système d'information sur lequel repose le télé-service à homologuer. Ce dossier peut contenir, en fonction de leurs pertinences au regard du contexte et de la complexité du système, des éléments organisationnels et techniques divers comme : L'existence d'un référentiel de sécurité, un document présentant les risques identifiés et les objectifs de sécurité, un journal de bord de l'homologation,...

La décision d'homologation de sécurité RGS, dite « attestation formelle » :

Arbitrage positif ou négatif, avec ou sans réserve, concernant la mise en production du ou des téléservices concernés, émis après analyse du dossier d'homologation. Cette décision est validée par l'autorité d'homologation.

DESCRIPTION DE LA DÉMARCHE D'HOMOLOGATION RGS

La démarche d'homologation doit s'inscrire dans un processus itératif d'amélioration continue de la sécurité. Il est préférable et plus efficace de la démarrer avant les phases de développement et d'intégration d'un nouveau service, même si ce dernier est déjà opérationnel, les objectifs de l'homologation restants les mêmes.

Elle a pour objectif de valider les conditions de sécurité d'un téléservice avant sa mise en production.

Selon leurs environnements, leurs maturités et/ou les risques résiduels, les homologations sont prononcées pour une durée de 1, 3 ou 5 ans.

La décision d'homologation peut comporter une réserve pour permettre la mise en place de mesures de sécurité nécessaires et proportionnées afin de réduire certains risques résiduels jugés encore important.

- Si certaines mesures de sécurité correctives ne peuvent être mises en place à courts termes, il est impératif de spécifier dans la décision d'homologation que la mise en place de ces mesures sera progressive, planifiée et suivie selon la durée de l'homologation. Elle doit commencer dès la date de publication de la décision.

Si des changements dans les architectures, infrastructures ou applicatifs sont suffisamment conséquents pour modifier le périmètre d'origine, alors la commission d'homologation devra à nouveau se réunir pour soumettre une révision de l'homologation précédemment prononcée.

Il existe un certain nombre de conditions de suspension ou d'annulation de l'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.

Si l'autorité d'homologation considère que les conditions ne sont pas réunies pour une homologation, la meilleure solution est de refuser l'homologation, ayant pour effet une annulation de la mise en production du téléservice.

Si cette possibilité n'est pas envisageable, il est toujours possible de prononcer une autorisation provisoire d'emploi (APE) pour une durée courte (3 ou 6 mois), assortie de conditions strictes et d'un plan d'action précis, destiné à supprimer ces risques trop élevés devant être réalisé durant le temps de l'APE.

PROPOSITION DE CONSTITUTION DE LA COMMISSION D'HOMOLOGATION

Dans ce cadre, et afin que la Ville de Clermont-Ferrand soit en conformité avec la réglementation, il est nécessaire de procéder :

- D'une part, à la désignation de l'autorité d'homologation de sécurité des systèmes d'information de la Ville,
- d'autre part, à la création de la commission d'homologation.

En complément, en fonction du niveau de sécurité requis pour le système d'information concerné et/ou d'un besoin spécifique identifié, le responsable du processus d'homologation (le

RSSI), désigné par l'autorité d'homologation, pourra compléter cette commission avec des membres occasionnels qui seront consultés, chacun en ce qui le concerne, sur le dossier d'homologation.

Ces membres occasionnels pourront être notamment des représentants d'autres directions de la Ville, concernées par le système d'information à homologuer (Chef de projet du service utilisateur, Direction des relations humaines, Direction de la Culture…) ou des prestataires informatiques de ces Directions (hébergeur, développeur et chargé de maintenance d'applications, consultants…).

Compte tenu des ces éléments, il vous est proposé en accord avec votre commission :

- De désigner en tant qu'autorité d'homologation de sécurité des systèmes d'information de la Ville de Clermont-Ferrand : La Directrice Générale des Services de la Ville de Clermont-Ferrand.

Cette autorité désignera un responsable du processus d'homologation qui mènera le projet d'homologation en son nom.

- De créer une commission d'homologation de sécurité des systèmes d'information de la Ville de Clermont-Ferrand composée des membres permanents suivants :

- le Directeur des Relations Usagers et de la Transformation Digitale ou son représentant
- le Directeur des Actions Juridiques et des Achats ou son représentant,
- le Responsable de la Sécurité des Systèmes d'Information ou son représentant,
- le Directeur des Usages Numériques,
- le Responsable du Centre de Services Technique ou son représentant,
- le Responsable du Centre de Services Applicatifs ou son représentant,
- le Délégué à la Protection des données ou son représentant,

ANNEXE - COMPOSITION DE LA COMMISSION D'HOMOLOGATION

Les acteurs de l'homologation sont :

• La maîtrise d'ouvrage (acteur complémentaire)

La maîtrise d'ouvrage représente les acteurs métier du téléservice concerné par l'homologation RGS, et assure la bonne prise en compte des contraintes liées à l'utilisation du système d'information. Elle joue un rôle-clé dans plusieurs étapes de la maîtrise des risques, y compris dans les arbitrages de leurs traitements.

• Le Responsable de la Sécurité du Système d'Information (RSSI)

Le RSSI est impliqué dans la démarche d'homologation. Selon les cas, il peut être désigné responsable du processus d'homologation, chargé du secrétariat de la commission d'homologation ou être membre de droit de cette commission.

• Le Directeur des Usages Numériques (DSI)

Le Directeur des usages numériques, au-delà de ses missions de pilotage de sa direction, est l'interlocuteur privilégié des autres directions de la ville il est également le responsable des Centres de services Applicatifs et Techniques.

• Le Responsable du Centre de Services Techniques (exploitation du système)

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

• Le Responsable du Centre de Services Applicatifs (applicatifs du système)

Le responsable des applicatifs du système remplit le rôle fonctionnel. Il s'agit de l'entité gérant la ou les applications destinées à être homologuées.

• Le Directeur des Relations Usagers et de la Transformation Digitale (DIRUTd)

Il représente la direction en charge du projet Gestion de la Relation Usagers - GRU qui est le portail fédérateur des téléservices que souhaite offrir la ville à ses concitoyens. Il contient l'essentiel des services qui nécessitent ou nécessiteront que la commission se réunisse pour proposer des homologations RGS.

• Le Directeur des Actions Juridiques et des Achats (DAJA)

Son rôle est en premier lieu d'informer et de conseiller sa direction ainsi que tous les services concernés quant aux évolutions du droit, des normes, de la jurisprudence. Pour cela, il assure une veille juridique et réglementaire permanente, rédige des notes de synthèse.

• Le Délégué à la Protection des Données (DPO)

Le Délégué à la Protection des Données - DPD ou DPO (Data Protector Officer) est en charge du respect des règles de traitements des données à caractères personnelles - DCP. Il est mutualisé pour la ville de Clermont-Ferrand, la Métropole, le CCAS de Clermont-ferrand et les communes membres et leurs CCAS ayant souhaité mutualiser. Il est désigné par les Maires et les Présidents des collectivités comme DPO auprès de la CNIL.

• Les prestataires

En fonction de leur implication dans le projet et de leurs relations avec l'autorité administrative, 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 versés au dossier d'homologation ainsi que des réponses aux interrogations de la commission d'homologation.

• Membres occasionnels

Ces membres occasionnels pourront être notamment des représentants d'autres directions métropolitaines, concernées par le système d'information à homologuer (Chef de projet du service utilisateur, Direction des relations humaines, Direction de la Culture…) ou des prestataires informatiques de ces Directions (hébergeur, développeur et chargé de maintenance d'applications, consultants…) pouvant apporter un éclairage complémentaire sur les téléservices concernés par l'homologation de sécurité.

DELIBERATION

Après en avoir délibéré, les propositions mises aux voix sont adoptées à l'unanimité.

Pour ampliation certifiée conforme.

Fait à Clermont-Ferrand, le 12 JAN. 2022

Pour le Maire et par délégation,
L'Adjointe,

Anne-Laure STANISLAS