

## 1. AUDIT / CONTRÔLE

### 1.3 Point cybersécurité et plan de remédiation ACPR

Annexe 1.3

**RAPPORTEUR :** Le Directeur Général

Par courrier du 28 mars 2025, l'ACPR nous a adressé la lettre de suite au rapport d'inspection de M. Delavis sur la gestion des risques informatiques de la caisse de Crédit Municipal de Nantes. Le 4 avril 2025, cette lettre a bien été transférée à la Présidente de notre Conseil d'Orientations et de Surveillance (COS) ainsi qu'à tous les administrateurs. Par courrier daté du 27 mai 2025, nous avons communiqué nos réponses en complétant l'annexe de la lettre de suite du 28 mars 2025.

Depuis le 27 mai 2025, la lettre de suite, ainsi que notre réponse, ont été présentées à la réunion du COS du 28 mai 2025. Un nouveau point d'avancement a également été réalisé lors du COS du 22 septembre 2025.

Par courrier en date du 7 novembre 2025, nous avons informé l'ACPR de la suite de nos avancées, et plus particulièrement de celles pour lesquelles un délai au 31 octobre 2025 avait été fixé. Pour synthétiser nos réponses détaillées développées au sein de l'annexe 1.3, je vous propose de faire un point sur les principales actions menées depuis le 27 mai 2025 (I-), puis de vous présenter l'avancement du plan de remédiation(II-), avant de terminer par vous indiquer, constat par constat, les réponses apportées au 31 octobre 2025 aux demandes de mesures correctives émises dans la lettre de suite(III-).

#### **I- Principales actions menées depuis le 27 mai 2025**

Depuis notre dernier courrier, les principales avancées sont les suivantes :

- Adoption par le GIE d'une PSSI et d'une charte informatique de groupe basées sur la PSSI et la charte informatique nantaises ;
- Mise à jour de la PSSI nantaise et de la charte informatique nantaise pour mise en cohérence avec la PSSI de groupe et la charte informatique de groupe adoptées par le GIE ;
- Refonte de notre plan d'urgence et de poursuite d'activité (PUPA), ainsi que de ses annexes que sont les plans de continuité des opérations (PCO) de chaque service :
  - o Ce PUPA a été mis à jour pour être conforme au règlement DORA ;
  - o Ce PUPA comporte un bilan d'impact sur les activités (BIA) ;
  - o Ce PUPA comporte un ordre de reprise des activités tiré du BIA suscité ;
  - o Ce PUPA comporte une mise à jour des analyses de risques de chaque scénario ;
  - o Ce PUPA comporte des délais de gestion de crise revus : durée maximale d'interruption acceptable (DMIA), objectif de délai de reprise (RTO), délai maximal de reprise technique prévu (DMRP), point de récupération des données (RPO) ;
  - o Ce PUPA comporte des réponses aux scénarios d'indisponibilité de certains prestataires ;
  - o Ce PUPA comporte des réponses renouvelées et détaillées à différents scénarios de cyberattaques ;
  - o Ce PUPA comporte un plan de tests annualisé.

- Création d'un plan de maintenance des matériels ;
- Durcissement de chacun des postes de travail du CMN ;
- Déploiement de l'authentification renforcée sur plusieurs applicatifs du CMN, dont le portail micro-crédit ;
- Mise à disposition des collaborateurs d'un coffre-fort de mot de passe certifié par l'ANSSI ;
- Recrutement d'un RSSI externalisé pour le GIE CM Services en remplacement de l'ancien salarié remplissant cette fonction ;
- Signature par le GIE CM Services d'un contrat permettant la mise à disposition en cas de besoin d'une équipe de réponse à incident (CSIRT).

## II- Avancement du plan de remédiation

Chacune de ces actions, et d'autres encore, ont permis un avancement significatif du plan de remédiation. Au 31 octobre 2025, au sein du **plan de remédiation** construit à la suite du contrôle ACPR initial, les actions à la charge du CM Nantes sont réalisées à hauteur de **87 %** (au 27 mai 2025, le taux d'avancement était de 57%). Il est précisé que les actions intégrées à ce plan de remédiation, et relatives aux constats n° 1 (Gouvernance), n° 6 (dispositif de maîtrise des risques) et n° 7 (formation et sensibilisation) sont réalisées à 100 %.

Au sein de ce **plan de remédiation**, et toujours au 31 octobre 2025, les actions à la charge du **GIE CM Services** sont réalisées à hauteur de **62 %** (au 27 mai 2025, le taux d'avancement était de 52%). Il convient toutefois de noter que le plan de remédiation tel que construit à la suite du contrôle ACPR comprenait 128 actions à mener à la charge du GIE CM Services. Le plan de remédiation actuellement suivi par le GIE comporte, non pas 128, mais 250 actions à mener. Le GIE CM Services a en effet intégré à son plan de remédiation les résultats d'autres audits, dont notamment celui de la société KPMG. Le pourcentage d'avancement ci-dessus indiqué (62%) est calculé sur la base de 250 actions. Si l'on se réfère aux seules **128 actions issues des constats de l'ACPR** lors du contrôle initial, le taux de réalisation est, selon les informations transmises par le **GIE**, de **81%**.

Dans le cadre de la maîtrise de ses externalisations, le Crédit municipal de Nantes prévoit d'auditer le plan de remédiation tel que présenté par le GIE CM Services pour en vérifier l'exactitude ; et ce avant le 30 avril 2026. A date, la première phase de l'audit a été réalisée, nous en avons débattu en comité IT et nous reviendrons vers le CAR et le COS à ce sujet.

## III- Etat des réponses apportées aux demandes de mesures correctives émises dans la lettre de suite

### Constat n°1 : Gouvernance

Le Crédit municipal de Nantes considère avoir tenu l'ensemble de ses engagements relatifs au constat n°1 dans la mesure où sa gouvernance est désormais véritablement impliquée dans les sujets IT, les sujets cyber, et le suivi des risques liés à l'informatique et aux prestations externalisées.

### **Constat n° 2 : sécurité du système d'information**

Au 31 octobre 2025, le Crédit municipal de Nantes considère avoir répondu aux demandes de mesures correctives formulées par l'ACPR dans la lettre de suite au stade du constat n°2. En effet, le Crédit municipal de Nantes a désormais terminé de définir et déployer une politique de sécurité des systèmes d'information. Le Crédit municipal de Nantes a également terminé de mettre en œuvre un jeu de contrôles permettant de réduire les risques découlant des manquements identifiés par l'ACPR.

Pour autant, le Crédit municipal de Nantes demeure déterminé à mener à leur terme les projets en lien avec le constat n°2 et listés dans son plan de remédiation. A ce stade, le bloc « constat n°2 » du plan de remédiation est réalisé à hauteur de 93%. La finalisation des projets en cours listés dans l'annexe 1 permettra d'obtenir un taux de réalisation à hauteur de 100%. Le Crédit municipal prévoit de boucler ces projets avant le 30 avril 2026.

Enfin, comme indiqué par ailleurs, le plan de remédiation deviendra, par l'ajout de projets nouveaux permettant d'augmenter le niveau de cybersécurité, un plan d'amélioration continue qui permettra au Crédit municipal de Nantes de se maintenir constamment au niveau des meilleures pratiques de sécurité.

### **Constat n° 3 : encadrement des prestations externalisées**

Comme annoncé en mai 2025, la finalisation de la mission externalisation demeure en cours au 31 octobre 2025. Néanmoins, de lourds chantiers sont d'ores et déjà lancés, notamment la renégociation des contrats avec l'aide du cabinet EY Avocats. Le Crédit municipal de Nantes maintient son engagement de terminer ce projet au 30 avril 2026.

### **Constat n° 4 : contrôle du GIE et de ses sous-traitantes**

La Caisse de crédit municipal considère être désormais en maîtrise de son prestataire le GIE CM Services et entend désormais travailler à maintenir son niveau d'exigence vis-à-vis de celui-ci. A ce titre, le Crédit municipal de Nantes prévoit d'auditer le plan de remédiation tel que présenté par le GIE CM Services pour en vérifier l'exactitude ; et ce avant le 30 avril 2026.

### **Constat n° 5 : continuité des activités**

Le Crédit municipal de Nantes considère avoir répondu à la première demande de mesure corrective issue du constat n°5 et énoncée par l'ACPR ; à savoir la mise à jour du plan d'urgence et de poursuite de l'activité. Cette demande avait pour échéance le 31 octobre 2025 ; date respectée par le Crédit municipal de Nantes.

Le Crédit municipal de Nantes demeure déterminé à répondre à la seconde demande de mesure corrective issue du constat n° 5 et énoncée par l'ACPR dans sa lettre de suite ; à savoir la réalisation de tests permettant de vérifier la capacité effective de mettre en œuvre le PUPA mis à jour. Cette seconde demande a pour échéance le 30 avril 2026 ; date que le Crédit municipal de Nantes prévoit de respecter. Pour ce faire, le test de restauration de l'environnement IBMI déjà réalisé sera complété par la réalisation du plan de test intégré au PUPA mis à jour, ainsi que par un test de restauration de l'ensemble des activités du GIE CM Services à partir du serveur de secours.

### **Constat n° 6 : dispositif de maîtrise des risques IT**

Le Crédit municipal de Nantes considère que, concernant les obligations issues de la lettre de suite et relatives au constat n°6, il a désormais répondu aux différentes remarques et demandes de l'ACPR. Il continuera de veiller à faire mettre en œuvre des contrôles effectifs sur les aspects IT et cyber.

### **Constat n° 7 : formation et sensibilisation**

Le Crédit municipal de Nantes considère qu'il aura rempli ses obligations issues de la lettre de suite et relatives au constat n°7 de l'ACPR à la date du 31 décembre 2025 au plus tard. Bien entendu, les attestations de présence aux formations programmées au mois de décembre 2025 seront communiquées courant décembre à l'ACPR.

En synthèse, nos avancées peuvent être présentées comme suit :

	Réponse du CMN aux demandes de mesures correctives de la <u>lettre de suite</u>	Echéances <u>lettre de suite</u> ou échéance sollicitée (*)	Taux de réalisation du <u>plan de remédiation</u>
Constat n°1	Terminé	31/10/2025	100%
Constat n°2	Terminé	31/10/2025	93%
Constat n°3	En cours	30/04/2026 (*)	56%
Constat n°4	Terminé	31/10/2025	81 % (GIE CM Services)
Constat n°5	En cours	31/10/2025 et 30/04/2026	83%
Constat n°6	Terminé	30/04/2026	100%
Constat n°7	Très avancé	30/06/2025 et 31/12/2025	100%

Notre sentiment global est que nous avons pu progresser rapidement, nous sommes en bonne voie pour l'échéance finale au 30 avril 2026. Nous notons aussi qu'un véritable changement de mentalité et de posture des différents acteurs est en train de s'opérer à la fois au sein du Crédit municipal de Nantes, mais aussi au sein du GIE CM Services et dans l'ensemble des caisses adhérentes.

Pour autant, nous restons concentrés sur la finalisation de nos actions ; en particulier sur les avenants contractuels à valider avec nos différents prestataires.

Enfin l'audit réalisé sur le plan d'actions du GIE annonce quelques sujets ponctuels qui seront probablement en retard pour le 30 avril. Nous entrons dans une phase d'échange avec la direction du GIE et leur RSSI pour avoir une bonne visibilité sur les points concernés, redéfinir les nouvelles cibles et en informer l'ACPR.

**Le Conseil prend acte de cette information.**

**NON TRANSMIS AU CONTROLE DE LEGALITE**