

# CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES (CCTP)

Audit technique relatif aux systèmes informatiques

## 1 – PRESENTATION DU COMMANDITAIRE

.....

.....

.....

.....

.....

## 2 - FONDEMENTS DU PROJET

### 2.1 - But du projet

La personne publique confie au soumissionnaire qui l'accepte, le soin d'assurer un audit technique informatique auprès de la Direction des systèmes d'information (DiSI).

Le soumissionnaire se chargera, en partenariat avec la DiSI, d'effectuer un diagnostic et, ce faisant, des préconisations sur les investissements nécessaires à court et long terme dans le cadre d'ajustements indispensables pour un fonctionnement optimisé et d'évolutions futures à programmer pour s'adosser à un futur schéma directeur numérique.

Il s'agit précisément d'établir un état des lieux, définir des points techniques à améliorer et proposer des recommandations ou scénarii d'évolutions sur trois aspects précis : réseau, applicatif et parc informatique.

### 2.2 - Personnes et services impliqués dans les enjeux du projet

Les personnes impliquées par la démarche sont le Directeur de la DiSI et les responsables de chaque Centre de la DiSI ainsi que le responsable de la sécurité du SI (Cf. Organigramme Joint) :.....

## 2.3. Périmètre de l'analyse

### 2.3.1 - Les aspects réseaux

#### 2.3.1.1 - Les sites et leur interconnexion

Cf schéma

.....

.....

.....

.....

.....

.....

.....

.....

#### 2.3.1.2 - Les bâtiments et leur interconnexion

Le principe général du câblage inter-bâtiments du site est basé sur un ensemble de fibres optiques doublées pour chaque bâtiment.

Liste des bâtiments raccordés:

.....

.....

.....

.....

.....

.....

.....

Ci-dessous le schéma d'architecture des fibres :

.....

.....

.....

.....

.....

.....

.....

### 2.3.1.3 - Le câblage des bâtiments

Chaque bâtiment a la même infrastructure de câblage.

Un local technique d'entrée de bâtiment se situant au rez-de-chaussée. Ce local relie chaque étage via un lien fibre 1Gb/s. Dans chaque étage nous trouvons un voire 2 locaux techniques.

Chaque local technique comprend des baies informatiques contenant les bandeaux de fibres optiques, des platines RJ45, ainsi que du matériel actif. Les switchs sont ensuite cascades via des liens Ethernet cuivre à 100Mb/s. Le matériel actif est constitué de matériel 3Com et Cisco.

Le câblage terminal (du local technique d'étage au poste de travail) est assuré par des liaisons cuivre à connectique rj45. Le débit final de l'utilisateur étant de 10 ou 100 Mb/s et évolue vers du Gb/s.

Tous ces locaux sont connectés « en étoile » sur l'entrée de bâtiment.

Exemple de raccordement :

.....

.....

.....

#### 2.3.1.4 - La connexion logique

Le premier élément de séparation des différents groupes d'utilisateurs est l'utilisation de VLAN. L'ensemble du matériel actif du réseau supporte cette technologie.

La technologie VLAN étant présente sur tout le site central et tous les sites distants, chaque port (point de connexion) de chaque matériel de la dorsale peut être affecté à un VLAN particulier.

La sécurité globale d'un VLAN est assurée par des filtres positionnés (listes de contrôles d'accès) par le matériel qui en effectue le routage (routeur, pare-feu...) de/vers l'extérieur : autres VLAN, autres réseaux...

### 2.3.2 - Les aspects applicatifs

#### 2.3.2.1 - Les applications métiers

Le pouvoir adjudicateur gère une vingtaine d'applications métiers dont les principales sont :

.....  
.....  
.....  
.....  
.....  
.....  
.....

Intégrées majoritairement dans une architecture n-tiers, ces applications exploitent Oracle Database, et pour quelques exceptions MySQL. Elles sont également exploitées dans le cadre d'un cluster « gestion » de lames serveurs IBM.

#### 2.3.2.1 – Les applications numériques

Les applications numériques métier :

Elles sont accessibles par le biais d'une authentification centralisée (SSO) et regroupe les services suivants :

- un service de mail

- des outils collaboratifs divers : agenda, gestion de tâches, carnet d'adresses, espaces de stockage,...
- une plateforme de certification C2I
- une plateforme collaborative
- une gestion de son profil
- des outils spécifiques
- un fil de nouvelles
- des informations utiles et des documentations générales
- un accès en lecture aux informations de réservation des salles
- des formulaires de demandes d'assistance

Tous ces services sont hébergés sur une infrastructure de serveurs en grande partie virtualisés sur l'environnement VMWARE, gérés de manière autonome par le CENUM. Ils s'appuient sur un ensemble de services système : annuaire LDAP, Authentification SSO, services DHCP, Mail Postfix, Samba, Apache, Mysql, Nagios,...) Elles sont également exploitées dans le cadre d'un cluster de serveurs plats et lames.

Les applications numériques transversales :

Ces applications sont utilisées soit par un service en particulier soit par toute la structure. Il s'agit de :

- d'applications spécifiques au service logistique
- un service de trombinoscope
- une application de gestion de la reprographie (à venir)
- une application de gestion du groupe logiciel

...

### 2.3.3 - Les aspects matériels

#### 2.3.3.1 - Les serveurs

La personne publique exploite .... serveurs essentiellement de type ...

... % de ces serveurs sont rackés dans quatre baies réseaux.

### 2.3.3.1 - Les micro-ordinateurs

- Le parc informatique administratif

La DiSI gère environ ... postes informatiques intégrés dans un domaine Microsoft Active Directory dont .... ordinateurs portables.

La plupart des postes sont installés sous Windows XP, à quelques rares exceptions sous Windows 2000 et Windows 7.

- Le parc informatique métier

Il est composé de ... PC (... modèles différents) réparties dans ... salles.

La majorité du parc (... modèles) est plutôt ancien et n'a pas de disque dur. Les machines démarrent, en chargeant une image distante, sur Windows XP et Linux Mandriva 2007.

.... PC récents fonctionnent avec Windows 7 et Linux Mandriva 2011 (installation sur disque dur local)

### 2.3.4 – Les technologies spécifiques utilisées

Chacune de ces technologies spécifiques ont un référent désigné pour une meilleure exploitation et gestion des compétences.

La personne publique exploite :

- La virtualisation avec VMware

A ce jour, il existe ... machines virtuelles hébergées sur ... serveurs physiques (... lames et ... serveurs plats).

- Un système de création d'image avec HP Neoware Image Manager et Ghost

La personne publique utilise ces technologies afin de permettre de diffuser des systèmes d'exploitation et leurs applications à la demande sur des postes clients dans les salles dites informatiques.

... serveurs permettent la diffusion de ces images pour Windows et 2 pour Linux.

- Des Blades Centers

La personne publique possède ... Blades Centers IBM dans lesquels sont enfichées ... lames serveurs contenant la majorité de nos applications métiers et numériques.

- Les SAN

La personne publique dispose également de ... SAN IBM connectés aux Blades Centers IBM de type DS3400 et DS4200.

### 2.3.5 La politique de sécurité

Le RSSI a, dans sa mission essentielle de sécurité, d'opérer certains types d'actions :

- définir le périmètre de la vulnérabilité lié à l'usage des technologies de l'information et de la communication;
- de réaliser une politique de sécurité en formalisant les normes générales de sécurité qui s'appliquent à l'ensemble des systèmes et de son personnel
- de concrétiser une démarche sécurité dans le cadre d'un projet dans la mesure où chacun est concerné par sa réalisation
- d'effectuer une classification des ressources pour déterminer leur degré de sensibilité.

Recruté depuis peu, il a la responsabilité de produire deux documents :

- la politique de sécurité SI dans lequel sera relaté la transcription d'un travail de modélisation pour comprendre les risques et leurs impacts en des mesures concrètes de sécurité.
- le schéma directeur SI dans lequel sera relaté une vision à long terme (3 ans) et les orientations à suivre en matière de sécurité.

## **3 - CONTRAINTES SUR LE PROJET**

### 3.1 – Une durée maîtrisée

Un temps est imparti pour effectuer la prestation. La prestation se réalisera dans un délai maximum de trois à quatre semaines.

### 3.2 – Une compétence reconnue dans les technologies ci-dessus présentées et exploitées au sein de l'organisme

Les auditeurs devront maîtriser les technologies présentes chez la personne publique. Leur expertise devra être démontrée par une expérience appropriée dans un environnement informatique complexe et, le cas échéant, les certifications afférentes à ces technologies.

### 3.3 – La prise en compte d'étapes prédéfinies dans la démarche globale

La démarche sera obligatoirement encadrée par trois étapes à prévoir devant un comité de suivi:

1 – au lancement, une présentation de la démarche avec le déroulé des tâches, les étapes, des phases, les outils....

2 – mi prestation, une présentation sur l'avancée des travaux et les tendances déjà identifiées

3 – à la fin, une exposition des résultats et des recommandations préconisées en termes de forces, de faiblesses et d'actions correctives à engager rapidement.

Le comité de suivi sera composé :

- de représentants de la direction générale,
- de représentants de la direction administrative et financière,
- de représentants de la DiSI et correspondants informatiques.

### 3.4 – Des éléments nécessaires à inclure dans la réponse du soumissionnaire à cet appel d'offre

Dans la réponse à ce cahier des charges, devra obligatoirement comporter :

1 - une démarche précise incluant une feuille de route datée et prenant en compte le périmètre à traiter

2 – une description des outils utilisés et des tâches entreprises pour mener à bien l'étude à réaliser selon les trois aspects décrits dans le §4 de ce cahier des charges

## **4 - EXIGENCES DE LA PRESTATION**

### 4.1 - Portée du travail

L'opération d'audit sera constituée par une étude délimitée et discernable selon trois aspects :

1 - Etude et diagnostic de l'architecture globale informatique avec notamment l'examen des possibilités offertes pour l'utilisation des serveurs informatiques et du matériel de stockage

Cela portera à minima, sur le dimensionnement et la cohérence entre :

Serveurs/applicatifs/débit

Virtualisation/architecture matériel

Blades centers/SAN/réseau

Applicatifs/parc informatique

2 - Etude sur la sécurité informatique des serveurs et des postes de travail, et leur évolution

Cela portera à minima sur :

les accès distants,

les sauvegardes

l'analyse des outils mis en place pour assurer la sécurité du réseau et les mesures anti-intrusion

les configurations des postes clients et leur adaptation aux besoins des utilisateurs

3 - Etude sur l'appréciation de la qualité, de l'accès, de la disponibilité du réseau et des connexions internet.

La personne publique souhaite mesurer et valider la qualité de sa structure réseau, de son cœur de réseau et vérifier la performance réelle de ses liaisons (SDSL, Fibres Optiques...).

A titre d'exemple et sans que cela soit limitatif, les mesures et tests devront porter sur les éléments suivants :

Performances et qualité des réseaux WAN,

- Répartition et natures des flux passant à travers le réseau,
- Bande passante et capacité réelle avant saturation de chaque lien,
- Contrôles de charges sur les liens (avec différents scénarios de transferts de fichiers par exemple),

- Répartition des bandes passantes par rapport aux flux, y compris par plages horaires et hebdomadaires,

Performance et qualité du réseau LAN

- Qualité technique, QOS
- Contrôles des services présents,
- Fonctionnement en débit réseau des switches,
- Contrôle de la DMZ (structure, configuration, efficacité...),
- Mesures en vue de l'optimisation des serveurs en charge CPU / HD / RAM / Débit réseau.

En cas de détection d'anomalie, des diagnostics supplémentaires pourront être effectués afin d'en déterminer les causes (qualité du câblage, des antennes, disfonctionnement matériel ou logiciel, paramétrages...).

Pertinence de la mise en place / renforcement de la QOS : Gain attendu par rapport à la situation actuelle et éléments d'administration future (matériels, logiciels, formation, pérennité...)

## 4.2 - Engagements de la prestation

### 4.2.1 - Avancement du projet

Le soumissionnaire informera au fur et à mesure de l'avancement de sa mission le comité de suivi dans le cadre de la démarche globale proposée et validée lors de la réunion de lancement.

L'interlocuteur principal en tant que chef de projet sera le DSI pour mettre au point toutes les modalités nécessaires d'exécution prévues dans la démarche globale. Par ailleurs, les responsables de centre participeront selon les besoins exprimés par le soumissionnaire dans sa feuille de route.

Il devra rendre compte de l'avancée de ces travaux au comité de suivi comme mentionné dans le paragraphe 3.3.

Le comité de suivi sera composé :

- de représentants de la direction générale,
- de représentants de la direction administrative et financière,

- de représentants de la DiSI et correspondants informatiques.

#### 4.2.2 - Livrables attendus

Le rapport d'audit comprendra deux parties :

l'exposé du diagnostic effectué comprenant l'analyse de l'existant dans lequel sera présenté notamment un tableau synthétique relatant les différents aspects abordés au §4.1 ;

une description des recommandations ou scénarii portant sur :

les choix techniques et matériels, détaillés et chiffrés en coût à privilégier ;

les modifications des paramétrages à effectuer pour l'amélioration des performances de l'infrastructure informatique ;

les prescriptions sécuritaires à mettre en place ;

la mise en place éventuelle de technologies nouvelles.

Par ailleurs, ces recommandations ou scénarii seront différenciés selon des critères prédéfinis et pertinents comme notamment :

- la rationalisation de l'équipement ;
- la concordance avec des évolutions futures ;
- la fiabilisation pour la continuité des services ;
- la sécurisation des données ;
- l'optimisation de l'infrastructure technique.

Ils permettront de distinguer les solutions optimales, acceptables, et prioritaires avec une évaluation de leur efficacité et efficience.