DOSSIER 1 : INFOGÉRANCE

À l'aide des annexes 1 et 2 et en vous appuyant sur vos connaissances, vous répondrez aux questions suivantes :

1°) Quels sont les différents types d'infogérance ?

L'externalisation des systèmes d'information consiste à confier la responsabilité de tout ou partie du SI à un prestataire qui s'engage sur des objectifs et facture à l'entreprise, la gestion des ressources matérielles et des logiciels d'application ainsi que le personnel nécessaire.

L'externalisation repose sur un cahier des charges, document contractuel où est exposé le transfert des ressources humaines, des ressources et moyens de production, des éléments matériels et/ou immatériels... Le résultat à atteindre doit être bien défini. La démarche s'appuie sur une analyse des coûts et des avantages pour appréhender la valeur du nouveau modèle.

Cela va de la conception d'applications spécifiques à la prise en charge complète du SI, en passant par des prestations d'audit et de conseil.

L'externalisation peut avoir un cadre très large et assurer les missions de conception, de création, de suivi et d'amélioration. Le terme d'infogérance désigne de façon indifférenciée l'ensemble des modalités d'externalisation en matière de SI, alors que TMA (Tierce Maintenance Applicative) s'emploie pour désigner la prise en charge du fonctionnement d'une application.

Ainsi, le périmètre de l'externalisation peut inclure :

- la gestion des matériels et leur maintenance ;
- la prise en charge des réseaux informatiques, et éventuellement de télécommunications ;
- l'architecture générale du système informatique et la planification de ses développements ;
- la maintenance des applications existantes (TMA) ;
- la conception et le développement d'applications nouvelles ;
- …

Lorsque la prestation concerne la gestion de ressources matérielles, celles-ci peuvent être gérées sur site ou hébergées par le prestataire. Dans l'un ou l'autre cas, elles peuvent être soit propriété du bénéficiaire, soit du prestataire.

2°) Quel est l'intérêt du recours à l'infogérance ?

Dans le domaine SI comme dans d'autres, l'externalisation peut s'inscrire dans une démarche d'entreprise de recentrage sur le métier de base en concentrant ses efforts sur les ressources considérées comme fondamentales et porteuses d'avantages concurrentiels. Dans cette optique, l'entreprise externalise les activités secondaires pour lesquelles elle est peu efficiente et ne souhaite pas investir davantage pour le devenir.

Les compétences nécessaires dans le domaine des TI sont complexes et très évolutives. L'intérêt pour l'entité qui externalise est de bénéficier de l'expertise du prestataire basée sur l'expérience acquise auprès de ses différents clients. Le recours à un prestataire spécialisé et reconnu garantit de disposer des meilleures solutions et pratiques disponibles sur le marché, car le prestataire est confronté en permanence aux problèmes qu'il doit résoudre pour ses différents clients.

Cette solution permet de mieux maîtriser les coûts, ceux-ci étant négociés dans le cadre d'un contrat. Le prestataire est en mesure de proposer des coûts inférieurs à ceux d'une solution interne du fait des économies d'échelle qu'il réalise et de la capitalisation des connaissances liée à la spécialisation dans son domaine et à la richesse de l'expérience dans ce domaine.

L'externalisation permet de transformer des coûts fixes en coûts variables. Le prestataire peut adapter les ressources mobilisées en fonction du besoin du client, par redéploiement de ses moyens, aussi bien en termes de nombre de personnes qu'en termes de compétences.

L'incompréhension (latente ou explicite) DG/DSI peut aussi être un facteur d'externalisation. Elle donne plus d'indépendance vis-à-vis des informaticiens internes, apparaissant comme un groupe particulier et étant suspectés d'utiliser leur expertise pour s'octroyer des pouvoirs disproportionnés.

3°) Quelles peuvent être les difficultés rencontrées dans la mise en œuvre d'une solution d'infogérance ?

Les risques de l'infogérance sont ceux de l'externalisation en général, avec des spécificités liées aux compétences mises en œuvre et aux enjeux en terme de sécurité.

Comme pour toute externalisation, il y a un risque de perte de compétences. Disposer d'un service informatique interne présente l'avantage d'une meilleure maîtrise du SI. Les choix sont faits dans l'organisation, le suivi est permanent.

Il faut établir une distinction selon que l'externalisation porte sur des tâches courantes (maintenance de matériel, d'applications…) ou a pour effet de confier au prestataire des responsabilités essentielles (conception, évolution du SI…).

Du fait des enjeux stratégiques liés au système d'information, le client risque de se trouver en situation de dépendance par rapport au prestataire : difficultés à contrôler la qualité de la prestation (celui-ci peut limiter ses efforts avec un risque de dégradation de la qualité du service ou de dérapage des coûts) et à revenir en arrière ou changer de prestataire en cours ou en fin de contrat.

Le facteur coût, même s'il n'est pas toujours déterminant, entre en ligne de compte. Mais la comparaison entre le coût de la prestation réalisée en interne et le devis d'un prestataire externe est parfois incertaine du fait de la relativité des méthodes de calcul de coût et de la difficulté d'évaluation du contenu de l'offre externe. Il y a pour l'entité qui a recours à l'impartition un risque lié à l'asymétrie d'information sur le coût réel de l'opération et sur la qualité.

De plus, les personnes extérieures qui interviennent sur le système d'information peuvent avoir accès à des données sensibles. Cela nécessite de mettre en place des règles de sécurité spécifiques.

4°) Quels sont les impacts au plan humain de ce choix ?

Par ailleurs, du point de vue social, il peut être délicat de gérer des salariés qui travaillent ensemble ou les uns à côté des autres avec des statuts sociaux différents. L'externalisation peut aussi être mal perçue par les salariés de l'entité qui externalise et générer un conflit social.

Il ne faut pas confondre externalisation et délocalisation (transfert d'activité dans des pays à bas coût de main d'œuvre), cependant les deux vont parfois de pair.

Certaines organisations, après avoir externalisé, adoptent parfois une position inverse : le back-sourcing.

Cela consiste à reprendre en interne des activités jugées intéressantes à contrôler. Cette opération peut se faire soit par rupture du contrat d'externalisation soit à la fin normale de ce contrat. La prise en compte de la réversibilité dès le début du contrat est indispensable pour permettre la reprise éventuelle des activités externalisées, y compris pour les confier à un autre prestataire.

5°) Quelles vous semblent être les conditions de réussite d'un projet de ce type ?

Compte tenu des intérêts partiellement divergents des parties prenantes à la relation contractuelle, la préparation, la mise en place et le suivi de celle-ci constituent des impératifs pour toute opération d'externalisation des SI.

Une réflexion stratégique préalable est indispensable pour bien identifier les compétences clés et les activités potentiellement externalisables. Cette étude doit évaluer la qualité, l'efficience et le coût des solutions existantes (solutions internes).

L'organisation doit définir précisément les compétences qu'elle souhaite externaliser. Elle peut choisir de garder en interne de certaines activités. De plus, conserver la maîtrise des activités externalisées nécessite de disposer de compétences internes.

Externaliser nécessite de définir les prestations à fournir, les critères d'évaluation utilisés et rédiger un appel d'offres. Il faut ensuite analyser les réponses à l'appel d'offres (en particulier, les compétences des répondants) et négocier avec le prestataire retenu sur les termes du contrat :

- définition précise des prestations à fournir, le prestataire pouvant demander des ajustements par rapport à l'appel d'offres ;
- organiser la phase de transition (information des utilisateurs, transfert des actifs. mise en place du suivi de l'exécution des contrats...) ;
- définition des modalités de contrôle de la prestation et des sanctions éventuelles ;
- fixation des modalités de facturation, des conditions de révision ;
- possibilités de modifications du contrat pour introduire les changements nécessaires (changement technologique et changement dans les processus métiers) ;
- conditions de renouvellement, de réversibilité ;
- …

L'engagement doit reposer sur des responsabilités mutuelles définies et mesurables par des indicateurs.
Pour développer une relation stable entre les deux parties, il faut au préalable communiquer les bonnes données et avertir de tout changement.

L'entreprise doit suivre l'exécution du contrat dans le cadre de réunions périodiques et sur la base des indicateurs définis dans le contrat. Ceux-ci doivent être mesurables suivant des critères précis. Il peut être prévu une comparaison (*benchmarking*) avec les meilleures références du marché.

Les réunions doivent aussi permettre un transfert de compétences de façon que la capitalisation des connaissances liées à la gestion du système ne se fasse pas exclusivement chez le prestataire au risque d'une perte de compétences et d'une moindre maîtrise de la prestation (risque de comportements opportunistes du prestataire).

Il est indispensable de garder la maîtrise de la relation avec le prestataire afin de préparer l'échéance du contrat pour avoir la possibilité de poursuivre voire d'étendre le contrat avec le même partenaire, de changer de partenaire ou de réintégrer les activités externalisées.
Il faut mesurer périodiquement la possibilité de réalisation, le cas échéant, de la réversibilité afin que le transfert vers un nouveau Prestataire ou vers le CRD-VEGALIS puisse se faire sans rupture de qualité de service.

DOSSIER 2 : GESTION DE LA PERFORMANCE

À l'aide des annexes 1 et 2 :

1°) Proposez une typologie des principales catégories d'indicateurs envisageables dans le cas étudié.

Le contrôle des systèmes d'information s'inscrit dans différentes perspectives :

- perspective d'efficience = résultats / moyens utilisés ; on trouvera ainsi des mesures simples de productivité directe par rapport d'un résultat aux ressources consommées ;
- perspective d'efficacité où l'on rapproche des résultats et des objectifs ;
- perspective de satisfaction : vision de l'efficacité organisationnelle exprimée au travers des perceptions des utilisateurs.

La question de l'appréciation du fonctionnement du SI peut appeler plusieurs types de réponses selon les points de vue : techniciens SI, utilisateurs (à différents niveaux), direction générale...

D'autre part une distinction peut être établie suivant la nature des indicateurs et leur objet : indicateurs techniques, quantitatifs ou qualitatifs, indicateurs financiers, indicateurs d'efficacité et d'efficience.
Il en découle différents critères que l'on peut classer en :

- **Indicateurs techniques** (point de vue du technicien) : volume d'activité, temps de réponse d'un serveur, temps réel d'utilisation, taux de disponibilité, nombre de logiciels ou de fonctionnalités utilisés...
- **Indicateurs d'utilisation** (point de vue de l'utilisateur) : impact sur la performance individuelle (temps d'utilisation, temps de réponse d'une application, amélioration de la performance…) ;
- **Indicateurs de satisfaction** (point de vue de l'utilisateur) : traduisent la perception de l'utilisateur qui découle d'une comparaison entre les attentes de l'utilisateur (ce qu'il espérait retirer de l'usage du système) et les résultats obtenus par l'utilisation ;
- **Indicateurs sur la performance de l'organisation** (point de vue de la direction) : efficience générale, performance financière, avantage compétitif, flexibilité, création de valeur...).

2°) Proposez au moins 5 indicateurs, couvrant les différentes catégories et justifiez-les.

La proposition ci-dessous n'est pas exhaustive, le correcteur jugera de l'intérêt de la proposition du candidat.

Indicateur	Définition	Justification
Nombre d'incidents réseau	Nombre d'incidents dus à des performances réduites des ressources informatiques	Permet de mesurer sur une période le nombre d'incidents donc la fiabilité du système et d'observer l'évolution dans la durée.
Taux d'incidents réseau	Part des incidents réseau par rapport au nombre total d'incidents enregistrés	Permet de mesurer l'impact des incidents réseau par rapport à l'ensemble des problèmes de fonctionnement du SI (problèmes liés aux utilisateurs, aux postes de travail…)
Taux de disponibilité des statistiques	Pourcentage de respect des délais de disponibilité des statistiques	Permet de mesurer la capacité du prestataire à remplir ses obligations de reporting, condition nécessaire pour établir une relation de confiance.

Indicateur	Définition	Justification
Degré de satisfaction des utilisateurs des postes de travail	Indice de satisfaction des utilisateurs par rapport à leur poste de travail mesurée par des enquêtes sur un échantillon représentatif.	Permet de mesurer l'orientation client du service fourni par le prestataire
Degré de satisfaction des utilisateurs du centre de services	Répartition (en %) des utilisateurs ayant eu recours au centre de services en fonction de leur satisfaction.	Permet de mesurer la façon dont les utilisateurs perçoivent les prestations du centre de services en termes de délai, de qualité...

3°) Préciser quelles sont les différentes composantes du coût d'un poste de travail.

Il faut prendre en compte l'ensemble des coûts liés à l'acquisition et à l'utilisation d'un poste de travail, incluant tout l'environnement nécessaire à son bon fonctionnement, pendant toute sa durée de vie :

➢ **Coûts directs**

- Les coûts, sous forme de dotations aux amortissements essentiellement, des matériels nécessaires (stations de travail, imprimantes, portables, périphériques, matériels d'infrastructure : serveurs, cartes de connexion, composants actifs...) ;
- Les coûts des licences des logiciels (système d'exploitation, outils bureautiques, messagerie, navigateurs, applications...) ;
- Les coûts de gestion des postes (prévision, acquisition, test, déploiement, sauvegarde, maintenance), cf. projet d'appel d'offres, cycle de vie des biens avec répartition des tâches entre DSI et infogérant ;
- Les coûts de mise au rebut (s'agissant d'un centre de recherches les disques durs doivent être détruits pour éviter des fuites) ;
- Les coûts des équipes internes d'exploitation ou de la part correspondante de l'infogérance ;
- Les coûts de support (centre de services, formation des utilisateurs...) ;
- Frais de télécommunications ;
- Autres coûts directs (consommables, documentation, énergie, place, etc.).

➢ **Coûts indirects**

- liés à l'utilisateur final (recours aux collègues ou résolution des problèmes sans aide, autoformation, développement d'applications personnelles).
- liés à la non optimalité du système (pertes de temps liées aux indisponibilités programmées ou non, défaillances des systèmes et applications, surcharge du centre de services…).

Certains organismes (Gartner…) proposent des méthodes de calcul du coût du poste de travail (TCO, *total cost of ownership*) et obtiennent des montants de l'ordre de 4 à 7 000 €, soit 10 fois le coût de la station de travail elle-même.

4°) En quoi la location des postes de travail pourrait-elle réduire ce coût ?

La location permet d'externaliser une partie des coûts liés aux postes de travail : le coût du matériel proprement dit et une partie des services liés à sa mise en service, sa maintenance et son élimination. Ces coûts vont être remplacés par un loyer dont le montant est négocié avec le prestataire sur la base d'une analyse précise des besoins, avec une plus grande flexibilité car le contrat peut prévoir des possibilités d'ajustement.

De plus, la location permet de remplacer des immobilisations par des loyers, donc évite de mobiliser des capitaux ce qui a un coût (intérêts si emprunt ou coût d'opportunité).

5°) Définissez le concept de « cloud computing » (informatique en nuage) et précisez si cela vous parait une solution alternative de réduction du coût des postes de travail, en justifiant votre réponse.

Définition : Il s'agit d'une forme d'infogérance où on loue un droit d'usage de ressources informatique de différentes natures et où les usagers ignorent où sont stockées leurs informations et les ressources qu'ils utilisent. Les ressources sont accessibles via Internet.

Le recours à des prestations externalisées apporte une visibilité des coûts pour une meilleure maîtrise et permet de bénéficier de l'expertise du prestataire pour obtenir un service de qualité au coût le plus juste. De plus, il est plus facile d'ajuster la ressource aux besoins par négociation avec un prestataire externe que lorsque la prestation est réalisée en interne.

Au-delà de l'infogérance, le cloud computing permet d'externaliser non seulement la gestion des ressources sur site mais de déporter celles-ci « dans le nuage ».

DOSSIER 3 : SÉCURITÉ INFORMATIQUE

A l'aide de l'annexe 2 :

1°) Après avoir rappelé ce qu'est un VLAN (réseau virtuel), préciser en quoi cela contribue à la sécurité.

Un VLAN (*Virtual Local Area Network* ou *Virtual LAN*, en français Réseau Local Virtuel) est une subdivision d'un réseau local regroupant un ensemble de machines de façon logique et non physique.

En effet dans un réseau local la communication entre les différentes machines est régie par l'architecture physique (les postes sont reliés à des commutateurs…). Grâce aux réseaux virtuels il est possible de définir une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses machines, numéros de port, adresses IP, etc.) de sorte que ces groupes de machine fonctionnent comme s'ils étaient sur des réseaux différents. Donc les machines concernées ne communiquent pas directement entre elles et doivent passer par un routeur ce qui permet de filtrer les communications entre les groupes de machines et limite les risques d'accès frauduleux ou involontaire à des données sensibles.

2°) Indiquer quels seraient les principaux points à aborder dans le document de synthèse concernant les mesures de sécurité, rédigé à l'intention du personnel, et expliciter chacun de ces points en quelques lignes.

Appréhender le risque : Quelles sont les menaces ?

La sécurité peut être appréhendée suivant trois dimensions :

- Confidentialité des informations : failles logicielles, possibilités d'écoute et d'interception, piratage pur et simple…
- Intégrité des traitement et des informations : maliciels (virus, vers, logiciels espion,…) , nuisance pure et simple (SPAM, canular, phishing…)
- Disponibilité : le déni de service ou la saturation…

➢ **Recommandations et précautions à prendre**

Le principal problème de sécurité est assis devant le clavier !

L'ingénierie sociale s'appuie sur l'absence de méfiance des utilisateurs pour contourner les protections.
L'intelligence économique permet d'obtenir des informations par l'écoute passive ou dans des situations en apparence anodines.
L'intrusion des outils grand public dans l'environnement professionnel (tablettes, mobiles…) est une nouvelle menace.
Le patrimoine scientifique et technique est une richesse qui doit être protégée.

➢ **Les aspects juridiques et réglementaires**

Rappel de la législation :

- Protection des personnes (CNIL)
- Infractions informatiques: intrusion, compromission … (LCEN - CP)
- Les droits d'auteur et le code de la propriété intellectuelle

➢ **La politique de Sécurité des Systèmes d'Information au CRD**

Principes et mise en œuvre de la politique de Sécurité des Systèmes d'Information au CRD
Brève présentation de la charte d'utilisation des moyens informatiques du CRD et du Plan de Sécurité des Systèmes d'Information

➢ **Le management de la sécurité au CRD**

Rôle des ASSI d'unité
Description des procédures et modalités d'accès au réseau (comptes utilisateurs…)
Classification des informations : confidentielle / non confidentielle.
Internet/Extranet/Intranet : modalités d'utilisation, niveaux de sécurité…

3°) Compte tenu de la nature de l'activité du CRD au sein du groupe, quels peuvent être les risques encourus par l'adoption d'une solution d'infogérance, pour la stratégie du groupe ?

La R&D est stratégique pour le groupe et elle est sensible en termes de confidentialité
L'externalisation de certains aspects du système informatique, notamment l'accès aux données sensibles put présenter un risque stratégique.