

DSCG 2012 UE 5 : l'infogérance de VEGALIS

Proposition de corrigé — non officielle. DSCG, session 2012, UE 5 Management des systèmes d'information : cas CRD-VEGALIS/Lorval, trois dossiers et deux annexes, durée 3 h, coefficient 1. Le pied de page comporte une mention 2011 discordante avec l'en-tête 2012.

[Sujet officiel](#) · [Annales de ce concours ou examen](#)

Dossier 1. L'infogérance

1. Les différents types

L'infogérance consiste à confier à un prestataire tout ou partie des activités informatiques. Elle peut être **globale** ou **partielle**, porter sur l'**infrastructure**, les **applications** ou une fonction comme le support. Elle peut être réalisée sur le site du client ou depuis un autre site. Ces distinctions se combinent : une maintenance applicative partielle peut être effectuée à distance.

Dans le cas VEGALIS, la prestation est réalisée sur site et couvre postes, périphériques, certains serveurs et applications, support et exploitation. Elle ne transfère pas toute l'autorité de la DSI. L'annexe 2 conserve notamment à celle-ci la gestion des niveaux réseau 3 et des serveurs DNS et AD en tant que machines ; l'infogérant réalise certaines opérations via les applications et procédures prévues.

2. L'intérêt pour le centre

Le centre peut disposer de compétences spécialisées et d'une organisation de support sans devoir les constituer entièrement en interne. Il peut contractualiser des niveaux de service, bénéficier d'une continuité des équipes et prévoir les coûts. La DSI peut se concentrer davantage sur les besoins de la recherche, la cohérence de l'architecture et le pilotage.

Ces avantages sont conditionnels. Le prestataire doit connaître les usages scientifiques et respecter les priorités des équipements critiques. L'externalisation d'une exécution ne supprime ni la responsabilité du centre, ni le travail nécessaire pour définir et contrôler la prestation.

3. Les difficultés possibles

Un périmètre imprécis favorise les renvois de responsabilité : un incident peut concerner une application infogérée et un serveur conservé par la DSI. Des volumes mal estimés, des coûts supplémentaires, une documentation insuffisante ou un prestataire difficile à remplacer peuvent compromettre le contrat.

Le cas révèle aussi un problème de visibilité : environ 200 appels mensuels ne donnent lieu qu'à 140 à 150 dossiers, notamment parce que certains appels rapides ne sont pas enregistrés et que les utilisateurs rappellent. Une mesure de la performance reposant seulement sur les dossiers sous-estimerait l'activité et masquerait les demandes répétées.

Le [guide ANSSI de 2010 sur l'externalisation](#) identifie les risques de perte de maîtrise, d'intervention distante et de mutualisation. Ils doivent être appréciés au regard du périmètre réel : une prestation sur site n'exclut pas des accès distants ou des sous-traitants.

4. Les impacts humains

Le changement modifie le rôle des équipes internes : davantage de pilotage, de contrôle et de coordination, parfois moins d'exécution directe. Il peut créer une inquiétude sur l'emploi, une perte de savoir-faire ou une difficulté à travailler avec des interlocuteurs nouveaux. Ces effets ne permettent pas de déduire automatiquement un licenciement ou un transfert de salariés : le sujet n'indique pas une telle décision.

Les utilisateurs doivent connaître le centre de services et les canaux admis. Le prestataire doit adapter son langage aux profils administratifs et scientifiques. La DSI, les correspondants informatiques et les ASSI conservent un rôle explicite ; les circuits de validation ne doivent pas être remplacés par des arrangements individuels.

5. Les conditions de réussite

Il faut définir le périmètre, les responsabilités, les horaires, les volumes et les niveaux de service ; sélectionner un prestataire compétent ; organiser la prise en charge ; conserver une équipe capable de piloter ; puis contrôler des indicateurs compréhensibles. Le contrat doit prévoir sécurité, confidentialité, sous-traitance, documentation et réversibilité.

L'annexe distingue une prise en charge à partir du 1er octobre 2012, une prestation à partir du 1er janvier 2013 et une réversibilité préparée avant la fin. Il faut lever l'ambiguïté entre les mentions de **42 mois** et de **39 mois** : les dates données correspondent à trois mois de prise en charge puis trente-six mois jusqu'au 31 décembre 2015, et non à trente-neuf mois après le 1er janvier 2013. Le cahier des charges doit préciser la période rémunérée et sa date de fin avant contractualisation.

Dossier 2. La gestion de la performance

1. Une typologie adaptée

Les indicateurs peuvent être regroupés en cinq catégories : **activité, qualité et délais, disponibilité, coûts, sécurité et satisfaction**. Ils doivent croiser volumes et résultats : résoudre peu de dossiers dans les délais n'est pas satisfaisant si une grande partie des demandes n'est pas enregistrée.

2. Indicateurs proposés et justification

Catégorie	Indicateur et calcul	Intérêt dans le cas
Activité	Nombre de demandes enregistrées par type et unité cliente	Suivre la saisonnalité et comparer la charge prévue à la charge réelle
Qualité	Dossiers résolus au premier contact / dossiers recevables	Limiter les rappels et l'attente, sans encourager une clôture prématurée
Délais	Demandes réalisées dans le délai contractuel / demandes terminées, par classe	Vérifier séparément les engagements de 2 h, 8 h ou plusieurs jours
Disponibilité	Temps de service disponible / temps de service attendu	Identifier l'impact sur les équipements critiques, selon leurs horaires
Coûts	Coût total de la prestation / nombre de postes pris en charge	Comparer des périodes et des périmètres équivalents
Sécurité	Comptes supprimés dans le délai prévu / départs signalés	Contrôler la gestion des accès dans un centre accueillant de nombreux temporaires
Satisfaction	Avis favorables / réponses à une enquête après résolution	Repérer les problèmes de communication ou de solution réellement utilisable

Chaque indicateur doit avoir une définition, une source de données, une fréquence et un responsable. Les exclusions et les suspensions de délai doivent être justifiées. Le nombre de répondants et le taux de réponse accompagnent une mesure de satisfaction. Aucun objectif chiffré supplémentaire n'est imposé par l'énoncé : ceux qui ne sont pas fournis sont à négocier, pas à inventer.

3. Le coût d'un poste de travail

Le coût complet comprend acquisition ou location, logiciels, déploiement et configuration, réseau, énergie, maintenance, support, mises à jour, sauvegarde, sécurité, immobilisation et fin de vie. Il faut aussi considérer le temps perdu par l'utilisateur pendant une panne ou une intervention. Le prix d'achat ne représente donc qu'une composante du coût total de possession.

Dans ce centre, les postes portables exigent notamment chiffrage et logiciels de mobilité ; les classes de service modifient les délais et les moyens à mobiliser. Une comparaison de coûts doit conserver un niveau de service comparable et ne pas compter deux fois une prestation déjà comprise dans le forfait.

4. L'intérêt et les limites de la location

La location peut étaler les paiements, simplifier le renouvellement et intégrer certaines opérations de maintenance. Des matériels homogènes réduisent parfois les variantes à administrer. Elle peut donc limiter certaines charges de gestion et éviter un parc vieillissant.

Elle ne garantit pas un coût inférieur. Il faut comparer la somme des loyers, les prestations incluses, les frais de restitution et les conditions de sortie à l'achat et à la maintenance équivalente. Le choix dépend aussi de la durée réelle d'utilisation. Une location courte pour des matériels conservés longtemps peut coûter davantage.

5. Le cloud constitue-t-il une alternative ?

Le cloud donne accès à la demande, par le réseau, à des ressources mutualisées et configurables. Le [NIST SP 800-145 de 2011](#) retient notamment libre-service, accès réseau, mutualisation, élasticité et mesure de l'usage. Il distingue des services d'infrastructure, de plateforme et de logiciel.

Une messagerie hébergée ou certaines applications en ligne peuvent réduire l'administration locale et déplacer des coûts vers un abonnement. Un poste léger peut suffire pour certains usages. Mais le centre conserve des équipements scientifiques, des logiciels particuliers et des exigences de confidentialité, de disponibilité et de connectivité. Tous les postes ne peuvent pas être remplacés par un accès web.

La décision nécessite donc un coût complet, des exigences de sécurité et un examen des données concernées, des performances, de la dépendance au fournisseur et de la réversibilité. Le cloud est une possibilité pour certains services, pas une réduction automatique du coût de chaque poste.

Dossier 3. La sécurité informatique

1. Le VLAN et sa contribution

Un VLAN est un réseau local virtuel : il regroupe logiquement des interfaces dans un domaine de diffusion distinct, indépendamment de leur proximité physique. Cette segmentation peut séparer des usages ou populations. Les échanges entre VLAN passent par un mécanisme de niveau 3, auquel on peut associer des règles de filtrage.

Un VLAN ne chiffre pas les données et ne remplace pas un pare-feu. Sans règles adaptées entre segments, le cloisonnement ne suffit pas à empêcher une communication indésirable. Dans l'annexe, la DSI conserve la définition des VLAN et la configuration des routeurs et du pare-feu ; l'infogérant réalise les opérations de niveaux 1 et 2 et l'affectation des adresses selon les procédures.

2. Document de sensibilisation proposé

Vos accès. Utilisez votre compte personnel, protégez vos identifiants et ne les communiquez pas. Une création, une modification ou une suppression de compte passe par le circuit prévu : demandeur, correspondant informatique, hiérarchie et ASSI. Les accès doivent correspondre aux fonctions et à la durée de présence.

Votre poste. Verrouillez la session en vous absentant. N'installez pas de logiciels ou de matériels non autorisés. Laissez fonctionner les dispositifs de protection et signalez les alertes. Les portables doivent utiliser le chiffrement et les outils de mobilité approuvés.

Les données de recherche. Conservez-les dans les emplacements autorisés, selon leurs règles de confidentialité et de sauvegarde. Ne les transmettez pas vers un service personnel ou un support inconnu. Vérifiez les destinataires et les droits de partage ; la possession d'un fichier n'autorise pas sa diffusion.

Les demandes et incidents. Contactez le centre de services par téléphone ou par le formulaire intranet. L'annexe exclut la messagerie comme canal de demande. Signalez rapidement la perte d'un équipement, une activité suspecte ou une erreur de transmission, sans chercher à dissimuler l'incident.

La sécurité physique et la mobilité. Protégez les équipements et documents contre les accès non autorisés. Utilisez les connexions prévues ; ne branchez pas un équipement personnel au réseau sans accord. En déplacement, ne laissez pas un portable ou un document sensible sans surveillance.

Vos interlocuteurs. Le correspondant informatique représente l'unité pour les besoins ; l'ASSI accompagne les règles de sécurité ; la DSI conserve le pilotage. Une demande urgente ne permet pas de contourner une habilitation ou de partager un compte.

3. Risques pour la stratégie du groupe

Le centre détient des résultats, projets et savoir-faire qui conditionnent son avantage concurrentiel. Un accès mal maîtrisé peut permettre une fuite, une altération ou une indisponibilité de ces informations. La perte de maîtrise d'un prestataire, sa défaillance ou une réversibilité insuffisante peut interrompre la recherche ou rendre une évolution très coûteuse.

Les réponses sont proportionnées aux risques : accès limités aux besoins, engagements de confidentialité, contrôle de la sous-traitance, traçabilité, sauvegardes vérifiées, documentation exploitable et tests de reprise. Le centre doit conserver la connaissance de son architecture et de ses données. Le prestataire peut apporter une compétence utile ; il ne doit pas devenir le seul acteur capable de comprendre ou de faire fonctionner le système.