GESTION DES RISQUES

L'INFOGÉRANCE

Externalisation de services informatiques et gestion des risques

Juin 2010

Groupe de travail CLUSIF

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11 rue de Mogador – 75009 PARIS

Tél. : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88 – e-mail : clusif@clusif.asso.fr

Web : www.clusif.asso.fr

en collaboration avec

ASSOCIATION POUR LE MANAGEMENT DES RISQUES ET DES ASSURANCES DE L'ENTREPRISE

Table des matières

Remerciements

Le **CLUSIF** et l'**AMRAE** tiennent à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Pour le CLUSIF

Vincent	**AUGER**	*Ministère de la Défense*
Jérôme	**GOSSÉ**	*Marsh*
Daniel	**LASSERRE**	
Michel	**PAILLET**	*Asip Santé*
Manuel	**PRIEUR**	*HP Enterprise Services*
Luc	**VIGNANCOUR**	*Marsh*

Pour l'AMRAE

Thierry	**BERNARD**	*Quadrige Société d'Avocats*
Hélène	**DUBILLOT**	*AMRAE*
Danielle	**MARSAL**	

Nous remercions aussi les adhérents du CLUSIF et de l'AMRAE ayant participé à la relecture.

Introduction

L'infogérance peut concerner toutes les entreprises quelles que soient leurs secteurs d'activité et leurs tailles. La volonté de confier à un partenaire extérieur la gestion de tout ou partie du service informatique peut constituer, soit une réponse face à une situation temporaire, soit un objectif fondamental de la stratégie de l'entreprise.

Le transfert des prestations vers un partenaire extérieur va modifier les risques de l'entreprise, leur perception ainsi que leur gestion.

Le but de ce document, dont le caractère n'est nullement exhaustif, consiste à apporter les bases nécessaires à une meilleure connaissance du sujet et quelques éclairages supplémentaires sur une pratique toujours en plein développement, surtout dans un contexte économique incertain.

Quatre chapitres composent la structure du document :

1. Définir l'infogérance

2. Rédiger les clauses du contrat d'infogérance

3. Connaître l'évolution des risques liés à l'infogérance

4. Transférer et financer les risques de l'infogérance

Ces chapitres sont complétés par des annexes : Glossaire, Normes de références et Clauses de sous-traitance en matière de protection des données personnelles (Source CNIL).

1. Définir l'infogérance

Définir l'infogérance, c'est en préciser les spécificités, le but, les contours et les limites.

L'infogérance ou *« Facilities Management »* est née aux États-Unis dans la deuxième moitié des années 1980, bien qu'existant auparavant sous des formes plus ou moins voisines comme le traitement à façon, le service partagé, l'infocentre, la fourniture d'énergie informatique.

On note, à partir de 1985, une conjonction de divers éléments : complexité des grands systèmes d'information et des grands réseaux de transport de données, mouvements de rapprochement et de fusion de grandes entreprises, pénurie de spécialistes, volonté des dirigeants de plus en plus nombreux désireux de recentrer leurs activités sur leur métier de base...

Ces facteurs ont ainsi accéléré le mouvement de délégation de l'informatique vers des sociétés spécialisées.

L'infogérance – ou externalisation de services informatiques – a ouvert progressivement son champ à des spécialités (par exemple : ASP *Application Service Provider*, en français FAH pour fournisseur d'applications hébergées) afin de répondre aux exigences de l'évolution des technologies de l'informatique. La notion d'infogérance s'inscrit dorénavant dans un périmètre de plus en plus large ; il s'agit ici d'en connaître l'essentiel. À noter qu'au Québec le terme usité est l'impartition.

2. Rédiger les clauses du contrat d'infogérance

L'infogérance ne fait pas l'objet de réglementation légale spécifique. Les dispositions du contrat d'infogérance relèvent de la liberté contractuelle, sous réserve de certaines réglementations de droit commun, par exemple le droit social. Pour ce qui concerne la partie purement conventionnelle, il existe néanmoins un certain nombre de clauses-types que l'on retrouve dans la plupart des contrats d'infogérance, issues de la pratique et des spécificités de cette prestation de service informatique.

Comme dans toute présentation de service informatique, le client doit être en mesure d'exposer dans un document usuellement dénommé « cahier des charges » les principales caractéristiques de son métier et de son système d'information. Le client doit également définir ses besoins à l'origine de la demande d'un service d'infogérance. Le cahier des charges est rédigé par l'entreprise (le client), le cas échéant, assistée par une société de conseil distincte du prestataire d'infogérance (mission d'assistance à maîtrise d'ouvrage).

3. Connaître l'évolution des risques liés à l'infogérance

La gestion des risques s'inscrit, le plus souvent, dans un concept plus global de *« risk management »* au niveau de l'entreprise. Cette gestion implique un processus d'indentification, d'analyse, d'évaluation, et le plus souvent, de traitement de ces risques, à partir d'une méthodologie appropriée.

L'informatique se situe dans ce cadre évolutif avec toutefois ses diverses spécificités liées à sa nature et à son rôle au sein de l'entreprise.

Dans le cadre de ce document, les risques seront étudiés selon 3 catégories :

- Les risques juridiques du fait de l'entreprise, du fait des salariés ;
- Les risques organisationnels liés à l'utilisation, à des fins malveillantes, des informations en circulation dans l'entreprise ;
- Les risques dits « de l'entreprise » ayant, par exemple, pour conséquence l'indisponibilité totale ou partielle des réseaux.

Selon les cas, les risques inhérents à l'entreprise (le client) seront analysés conjointement avec ceux du prestataire en infogérance. Tous les domaines de sécurité (physique, logique...) doivent être ainsi étudiés selon une finalité commune.

4. Transférer et financer les risques de l'infogérance

Après les phases d'identification, d'analyse et d'évaluation, si possible, le traitement s'impose par des mesures de prévention et de protection, et logiquement, après une étude de faisabilité, par des opérations de financement appropriées.

L'assurance est l'un des moyens de traitement du risque. Elle constitue une formule de financement généralement la mieux adaptée à toutes situations et aux attentes des parties : le client (l'entreprise) et le prestataire.

On distingue les risques de dommages et pertes – directes et indirectes - relatives aux biens et aux systèmes d'information des risques de responsabilité civile générale et professionnelle.

Les aspects « assurances » sont liés aux particularités du contrat d'infogérance, notamment en présence de clauses de renonciation à recours, de limitation ou d'exonération, en cas de responsabilité contractuelle.

I - L’infogérance, un domaine étendu

L’infogérance constitue un domaine essentiel de l’informatique et des métiers annexes. Comme dans d’autres domaines de l’informatique et des nouvelles technologies de l’information et de la communication, ce sont souvent des termes anglo-saxons utilisés pour désigner ce service, tels *« Facilities Management »*, qui, avec une idée de moyens et d’équipements, a été utilisé en premier lieu pour désigner la gestion, puis plus récemment le terme *« Outsourcing »* qui a été utilisé pour désigner une notion d’externalisation du service.

En pratique, on appelle infogérance l'externalisation d'une partie des services informatiques d’une entreprise (moyens matériels et/ou ressources humaines) , c'est-à-dire la possibilité de confier tout ou partie de la gestion du système d'information à un prestataire informatique tiers.

La prestation fait l'objet d'un document annexé au contrat, généralement dénommé « convention de service » (ou, en anglais, *Service Level Agreement*, abrégé en « SLA ») définissant les conditions opérationnelles auxquelles le prestataire s’engage et, plus globalement, le niveau de qualité de service attendue. Ce document est essentiel pour préciser les résultats attendus de la prestation sur la base d’indicateurs arrêtés d’un commun accord entre les parties (délais de réponse et de résolution du service de maintenance, disponibilité du service infogéré, temps de réponse,…).

L'infogérance a des avantages et des inconvénients.

Le principal avantage est que l’infogérance permet à l'entreprise de se centrer sur son cœur de métier et de confier la gestion de son système informatique à une société, possédant les compétences adéquates, capable de le maintenir 7 jours sur 7 et 24 heures sur 24 (selon la convention de service).

L‘inconvénient, même si celui-ci n’est pas toujours présent dans l’esprit des décideurs est le fait que l’entreprise pourrait dépendre d'un tiers, et ainsi perdre, en tout ou partie, un savoir faire technique (informatique) interne nécessaire à la maîtrise d’un outil stratégique dans l’exploitation courante de l’entreprise.

D'une manière générale l'infogérance est toujours choisie en connaissance des coûts complets (TCO, *Total Cost of Ownership*, en français coût total de possession). Cela inclut le prix du matériel informatique, des réseaux, du maintien des compétences des équipes informatiques et éventuellement du coût engendré par l'arrêt du service ou de sa mise à jour.

II - Les clauses du contrat d'infogérance – Guide de rédaction

II.1 - Avertissements

Le présent guide a pour objet d'exposer les principaux points d'attention pour la rédaction d'un contrat d'infogérance soumis au droit français ; il ne s'agit que d'un document type, et à ce titre, son application à chaque situation particulière nécessite une analyse métier et juridique préalable pour s'assurer de son adéquation et des modifications/compléments à lui apporter.

Comme pour toute prestation de service informatique, le client doit être en mesure d'exposer dans un document usuellement dénommé « cahier des charges », les principales caractéristiques de son métier et de son système d'information. Il en est de même de ses besoins à l'origine de la demande d'un service d'infogérance ; le cahier des charges est rédigé par l'entreprise, le cas échéant assistée par une société de conseil distincte du prestataire d'infogérance (mission d'assistance à maîtrise d'ouvrage, notamment dans la détermination des indicateurs de performance de l'infogérance).

Il est rappelé qu'il existe des normes concernant spécifiquement les prestations d'infogérance, qui restent cependant facultatives (ces normes peuvent néanmoins constituer une référence en cas de contentieux). Ces normes sont mentionnées en annexe I.

Il est indispensable que les aspects « assurances » fassent l'objet d'une étude préalable approfondie en explicitant les intérêts en jeu de chacune des parties et les solutions d'assurances les plus appropriées.

II.2 - Préambule

Le préambule du contrat d'infogérance comprend la présentation du client, du prestataire ; l'exposé des besoins du client ; un rappel de la connaissance par le prestataire du contexte du client, de l'analyse de l'existant ; un rappel des points critiques des besoins, de la prestation... ; un exposé de la proposition du prestataire.

- Présentation du client.

  Commentaire *: le niveau de connaissance technique du client au regard de l'objet du contrat, notamment l'existence et l'ampleur d'un service informatique interne, sont pris en considération en cas de contentieux avec le prestataire pour définir le niveau de son obligation d'information et de conseil contractuelle et précontractuelle.*

- Présentation du prestataire.
- Exposé des besoins du client (situation actuelle et des objectifs) / rappel de l'existence d'un cahier des charges (descriptif de l'existant, contraintes métiers d'exploitation, niveaux de performance, compatibilité des contrats informatiques en cours avec le passage en infogérance,..) et le cas échéant de l'appel d'offre réalisé. Il est souhaitable d'y annexer le cahier des charges.
- Rappel de la connaissance par le prestataire du contexte du client, de l'analyse effectuée par le prestataire de son existant et de ses besoins.

- Rappel spécifique des points critiques des besoins et / ou de la prestation / qualités attendues du prestataire et de la prestation comme conditions essentielles ayant déterminé le client à contracter.
- Exposé de la proposition du prestataire.

II.3 - Définitions

Voir glossaire en Chapitre V.

II.4 - Objet

Commentaire *: ne pas oublier de rappeler au début du contrat la signification des acronymes d'applications ou autres, y compris courants ou spécifiques au client.*

- Prestation de service du prestataire en qualité de maître d'œuvre, consistant en l'exploitation du système d'information du client tel qu'existant à la date du contrat et en la prise en charge de son évolution éventuelle conformément aux besoins du client.
- Exécution de prestations accessoires ou connexes (formation, assistance, plan de sécurité...).
- Prestation relative à la réversibilité pendant et au terme du contrat.
- Dans le respect des indicateurs de performance annexés au contrat, à titre d'obligation de résultat du prestataire.
- Au bénéfice dudit client, maître de l'ouvrage, en contrepartie de la rémunération visée au contrat.

II.5 - Obligations du prestataire / maître d'œuvre

Commentaire *: rappel des obligations générales, sachant que des clauses spécifiques développent certaines obligations particulières.*

- Obligation d'information, de conseil, de mise en garde, de maintien de l'équipe nécessaire et des compétences.

  Concernant l'obligation de maintien d'équipes compétentes, il est à noter qu'en matière de marchés publics, la réglementation prévoit expressément une telle obligation du prestataire (Article 5 « **Conduite des prestations** » du Cahier des Clauses Administratives Générales (« CCAG ») applicables aux marchés publics de prestations intellectuelles).

  Dans le cas où des personnes seraient nommément désignées et qu'elles ne seraient plus en mesure de remplir leurs missions, le titulaire devra en aviser immédiatement la personne responsable du marché et prendre toutes les dispositions nécessaires pour que la bonne exécution des prestations ne s'en trouve pas compromise.

  À ce titre, obligation lui est faite de désigner un remplaçant et d'en communiquer le nom et les titres à la personne responsable du marché dans un délai de quinze

jours à compter de la date d'envoi de l'avis dont il est fait mention à l'alinéa précédent.

Le remplaçant est considéré comme accepté si la personne publique ne le récuse pas dans un délai de deux mois à compter de la réception de la communication mentionnée à l'alinéa précédent. Si la personne publique récuse le remplaçant, le titulaire dispose de quinze jours pour désigner un autre remplaçant et en informer la personne responsable du marché. À défaut de désignation, ou si ce remplaçant est récusé dans le délai de deux mois indiqué ci-dessus, le marché est résilié dans les conditions prévues (article 39 des CCAG**)**.

- Maintenir des matériels / logiciels faisant l'objet de l'infogérance à titre d'obligation de résultat
- Respecter des indicateurs de performance définis dans le « contrat de service » (ou *« Service Level Agreement »)* (cf. annexe II)

II.6 - Obligations du client / maître d'ouvrage

- Rappeler la collaboration : mise à disposition des informations métiers et notamment de toute spécificité ou changement de la législation ou de la réglementation concernant son métier et pouvant entraîner des contraintes particulières pour le fournisseur.
- Rappeler également concernant la mise à disposition des informations relatives au système d'information en place, sous réserve de l'obligation de conseil du prestataire lequel doit également de son côté questionner le client sur toute précision spécifique utile concernant l'existant et les attentes de ce dernier.

II.7 - Documents contractuels

- Définir les documents concernés.
- Rappeller l'ordre de préséance (contrat / annexes).

II.8 - Phases / calendrier

- Décrire les phases d'exécution des prestations à réaliser par le prestataire (audit - en phase précontractuelle ou en phase contractuelle / définition de l'architecture / le cas échéant, commande de matériels et logiciels, installation / migration / recette du périmètre concerné par l'infogérance / production).
- Arrêter le calendrier de réalisation des prestations, recettes partielles et globales des lots.
- Prévoir des pénalités en cas de retard (pendant toute la durée du contrat, à chaque mise en production d'un lot).

II.9 - Comité de pilotage

- Désigner le nombre de personnes, leur qualité (technique, décisionnaire…).

- Définir la tenue des réunions : auteur et mode de convocation, fréquence, compte rendu (compte rendu contradictoire dont l'auteur est généralement le prestataire), modalités de validation du compte rendu.
- Suivre les missions : suivi et coordination technique, respect du calendrier et plus généralement du PAQ (« Plan d'assurance qualité »)/SLA, de la politique de sécurité, propositions techniques et d'organisation relative à la mise en œuvre du processus d'exploitation.
- Prévoir que le comité n'a pas de pouvoir de décision quant à la modification des prestations et des clauses du contrat.
- Prévoir une procédure interne de solution (recours aux décisionnaires de chaque partie au contrat), délai de résolution, par exemple en cas de blocage persistant du Comité de pilotage.

II.10 - Comité de direction

- Prévoir la composition du Comité de direction avec des représentants disposant d'un pouvoir décisionnaire et en précisant son rôle.
- Préciser la fréquence des réunions (de l'ordre d'une à deux par an)
- Stipuler qu'en cas de désaccord persistant du Comité de pilotage (ci-dessus), il sera prévu une procédure d'escalade vers un Comité de direction représentant les deux parties.

II.11 - Équipe du prestataire

- Engagement du prestataire de mettre en place une équipe dotée de la qualification et de l'expérience nécessaire à la réalisation de la mission.

  Commentaire *: de préférence joindre les CV de l'équipe pressentie afin d'avoir des précisions sur le niveau technique minimum requis pour les besoins de l'engagement sur la pérennité du niveau de service. En tout état de cause, ces CV ne seront qu'informatifs, ce qui permettra néanmoins d'avoir un niveau de compétence, de référence, en cas de remplacement de tout ou partie de l'équipe prévue initialement (cf. ci-après).Le cas échéant, préciser la langue d'exécution du contrat.*
- Engagement du prestataire sur la pérennité de l'équipe, sauf indisponibilité du personnel indépendante de la volonté du prestataire.
- En cas d'indisponibilité, engagement de remplacement du/des membres de l'équipe par des collaborateurs de niveau et expérience équivalents et dans cette hypothèse, sans incidence sur le calendrier et la qualité du service.

II.12 - Maintenance

Il convient d'identifier / définir au préalable le titulaire de la propriété et du droit d'usage des matériels et logiciels concernés.

- Le prestataire en tant qu'infogérant est par principe responsable de la maintenance (cf. obligation de maintien en conditions opérationnelles du service) en conformité avec les obligations de niveau de service (SLA/PAQ) du prestataire à l'égard du client.
- Si certains matériels / logiciels sont sous contrat avec le client directement, il convient de le rappeler et de prévoir que le prestataire représentera le client à l'égard du mainteneur ou que ces contrats seront résiliés et repris en direct par le prestataire. Un inventaire préalable des conditions contractuelles et financières de résiliation s'avère utile.
- Pour les matériels en cours d'amortissement et / ou en location, il est nécessaire de dresser un état préalable des conditions contractuelles et financières de résiliation.

  Commentaire *: Il est à noter que dans des cas spécifiques (par exemple, pour des logiciels spécifiques au métier du client), le client pourra préférer conserver la relation clientèle avec le mainteneur (pouvoir de négociation, retour d'informations en direct du mainteneur…), même si le prestataire demeure le représentant du client au niveau opérationnel quotidien.*

II.13 - Evolutions (matériel et logiciel)

- À l'initiative du prestataire :
  - Obligation du prestataire de proposer des évolutions permettant une amélioration du service.
  - Obligation pour le prestataire de soumettre au client un dossier de spécifications, un devis, une analyse d'impact (avantage / inconvénient de l'évolution aux plans opérationnel, technique et financier).
  - Liberté pour le client d'accepter ou refuser l'évolution (avec dans certains cas la possibilité pour le prestataire d'exclure sa responsabilité au cas où un dysfonctionnement résulterait du refus de l'évolution).
- À l'initiative du client :
  - Faculté pour le client de demander des évolutions (évolutions « métier », nouvelles fonctionnalités,…).
  - Obligation du prestataire de prendre en compte la demande et de proposer au client un dossier de spécifications, un devis, une analyse d'impact (avantage/inconvénient de l'évolution aux plans opérationnel, technique et financier).
  - Faculté pour le prestataire de déconseiller la mise en œuvre de l'évolution demandée ; si le client passe outre, le prestataire aura la faculté dans certains cas d'exclure sa responsabilité dans l'éventuelle dégradation de ses prestations.

>> Dans les deux cas : prévoir le préavis de demande d'évolution, les délais d'étude et modalités de contractualisation des conditions de réalisation de l'évolution.

II.14 - Prestations annexes

- Formation.
- Conseil (expertise technique spécifique…).
- Autres.

II.15 - Sous-traitance

- Liberté pour le prestataire de sous-traiter, sous réserve d'imposer à ses sous-traitants le respect de l'ensemble des obligations auxquelles est tenu le prestataire à l'égard du client (niveau de sécurité, confidentialité, assurance…).
- Préciser si le prestataire doit informer le client ou lui demander son autorisation.
- Maintien exprès du prestataire en qualité d'interlocuteur unique du client.

  Commentaire *: déclaration obligatoire du prestataire, en cas de marché public, des sous-traitants concernés par la prestation.*

II.16 - Prix

Le prix est un fixe ou un variable en fonction des paramètres prédéterminés.
Préciser l'indice d'actualisation (Syntec ou autres), les règles de facturation et de paiement des factures.

II.17 - Veille concurrentielle (« benchmarking »)

- Possibilité de prévoir une veille sur les tarifs pratiqués auprès des concurrents du prestataire pour le même type de prestation, soit pour l'ensemble de la prestation, soit pour les extensions de services.
- En cas d'écart prédéterminé (+/- x%), prévoir, soit une obligation de renégociation des conditions tarifaires du contrat, soit un ajustement en conséquence du prix du prestataire, soit la résiliation.
- Prévoir les modalités de la veille : devis ponctuels ou tiers expert désigné au contrat.

II.18 - Durée

- Durée déterminée, généralement en fonction de l'investissement du prestataire ; souvent de l'ordre de 3 à 5 ans, selon la nature des projets.
- Reconduction : tacite ou expresse (le cas échéant, obligation du prestataire de notifier le terme du contrat suffisamment tôt afin de permettre la mise en œuvre de certaines opérations et notamment la réversibilité).

II.19 - Résiliation

- Possibilité de prévoir une résiliation pour faute (éventuellement, « de droit » en cas de faute grave : manquement à une ou plusieurs obligations essentielles du contrat + manquement répété à une obligation non essentielle ; le cas échéant, préciser pour chaque partie le type d'obligations visées).
- Possibilité de résiliation unilatérale non fautive prévue au contrat.
- Possibilité de prévoir une indemnité contractuelle prédéterminée en cas de faute du prestataire (par exemple, prise en charge du coût de la réversibilité et autres dommages causés au client).

  Commentaire : *éviter la qualification de clause pénale qui est révisable par le juge conformément à l'article 1152 du code civil.*
- Possibilité de prévoir un préavis (de résiliation) : définir et organiser les durées de préavis en fonction des contraintes techniques et en concordance avec les autres clauses contractuelles (veille concurrentielle ou « benchmarking », réversibilité…).

II.20 - Protection des données / données personnelles

- Dès lors que le client demeure la personne définissant la finalité et les moyens des traitements sous-traités à l'infogérant, le client demeure responsable du respect de la réglementation relative à la protection des données personnelles faisant l'objet desdits traitements au sens de la loi « informatique et libertés » (loi n°78-17 du 6 janvier 1978 modifiée) ; les déclarations / autorisations des traitements auprès de la CNIL sont de la responsabilité du responsable du traitement.
- L'infogérant s'oblige au respect de la confidentialité des données personnelles du client ; voir la clause de confidentialité (modèle) recommandée par la CNIL jointe en annexe.
- Prévoir l'autorisation préalable du client pour tout traitement de données nominatives effectué hors de l'Union Européenne.

II.21 - Propriété intellectuelle

- Déclaration par le client de titularité des droits de propriété ou d'usage des logiciels / progiciels/matériels qu'il remet au prestataire.
- Engagement du prestataire de respecter les contrats / conditions d'utilisation des logiciels/progiciels/matériels du client – obligation d'utilisation aux seules fins de l'exécution du contrat d'infogérance.
- Déclaration par le prestataire d'être titulaire des droits de propriété ou d'usage des logiciels / progiciels / matériels qu'il met en œuvre et met à disposition du client pour l'exécution de l'infogérance.
- Garantie d'absence de contrefaçon des logiciels / progiciels / matériels (par le client, pour ceux mis à disposition du prestataire ; par le prestataire, pour ceux autres que ces derniers utilisés par le prestataire pour les besoins de l'infogérance).

- Cas des logiciels développés spécifiquement par le prestataire pour les besoins de l'infogérance : prévoir la faculté pour le client d'en acquérir les droits (y compris codes sources et documentations afférentes) au fur et à mesure de leur développement ou à l'issue du contrat d'infogérance (nonobstant les conditions générales du prestataire).

  Commentaire *: attention à la rédaction de cette clause qui doit être strictement conforme aux dispositions du code de la propriété intellectuelle. Ne peut être cédé que ce qui est expressément visé au contrat (préciser la durée, la nature des droits cédés, les modes d'exploitation, le territoire) ; la seule stipulation de la commande d'un logiciel, même réglée par le client, n'emporte pas cession des droits au profit de ce dernier, mais uniquement concession d'un droit d'utilisation à durée indéterminée.*

  Commentaire : *le cas échéant, en fonction de l'activité du client et de la nationalité du prestataire et/ou de ses sous-traitants, vérifier les risques potentiels de fraude en matière d'intelligence économique…*

II.22 - Sécurité / Prévention

Commentaire *: il peut être décidé d'imposer telle ou telle préconisation technique au prestataire en matière de sécurité (en référence à la politique de sécurité de l'entreprise)), mais dans ce cas des discussions pourraient naître, en cas de dysfonctionnements ultérieurs qui pourraient résulter directement ou indirectement de ces préconisations, sur l'étendue de la responsabilité du prestataire ; le prestataire reste néanmoins tenu (et responsable à ce titre) d'avertir le client des conséquences éventuelles de tels choix de sa part.*

- Le cas échéant, décrire le niveau de sécurité minimal souhaité par le client.
- Rappeler le devoir de conseil du prestataire sur l'existant et sur les évolutions, ainsi que son devoir d'alerte.
- Définir les conditions de sauvegarde et d'archivage (selon les besoins du Client).
- Sécurité physique (susceptible de concerner les locaux où s'exercent les activités du client et / ou du prestataire).
- Prévoir l'obligation pour le prestataire de concevoir et mettre en œuvre des mesures techniques et d'organisation en vue de prévenir notamment les risques d'incendie, de dégâts des eaux, électriques, d'intrusion et tout autre risque spécifique lié à la situation des locaux.
- Sécurité logique (susceptible de concerner le client et / ou le prestataire).
- Prévoir l'obligation pour le prestataire de concevoir et mettre en œuvre les mesures nécessaires pour assurer la sécurité du système informatique du client, des réseaux, propres, dédiés, partagés ainsi que des données confiées, en fonction du périmètre de responsabilité de chacun des intervenants (notamment, définition des règles d'accès au système informatique et aux données confiées, maintien en condition de sécurité).
- Mise en place d'indicateurs pour leur suivi régulier.
- Obligation d'information en cas d'incident de sécurité (criticité à définir).

II.23 - Plan de secours

- Engagement du prestataire sur les conditions de remise en état et de maintien d'une solution de secours opérationnelle pendant la durée du contrat.
- Engagement du prestataire en matière de gestion des sauvegardes et des archivages.
- Vérification périodique contradictoire, par le prestataire et le client du bon fonctionnement de la solution de secours mise en place (simulations).

II.24 - Audit

- Principe : possibilité pour le client de faire procéder à des audits sur les conditions d'exécution du contrat.
- Définir les conditions d'exercice de l'audit à convenir dans le contrat : conditions de mises en œuvre de l'audit (forme et délai de prévenance du prestataire), fréquence et périodicité, choix de l'auditeur, agrément du prestataire…), conditions financières (à la charge du client, ou le cas échéant du prestataire en cas de manquement constaté aux termes de l'audit).
- Définir le périmètre de compétence de l'audit - points susceptibles d'être audités.
- Définir la valeur et la portée du rapport d'audit (obligations résultant du rapport d'audit pour le prestataire : obligation de faire, conditions financières - à la charge du prestataire en cas de manquements constatés aux termes de l'audit -, fixation de délais d'exécution).

II.25 - Réversibilité

La prestation de réversibilité a pour objet d'assurer la reprise partielle ou complète du système d'information par le client ou par un nouveau prestataire. Il est essentiel d'en prévoir les conditions de réalisation entre les parties et, si possible, fournir un plan de réversibilité initial et de le mettre à jour périodiquement. Pour autant, à la signature du contrat d'infogérance, il n'est généralement pas possible de décrire précisément les opérations qu'il y aura lieu de mettre en œuvre pour pratiquer la réversibilité, dans la mesure où le système d'information a vocation à évoluer entre l'entrée en vigueur du contrat et son terme. En revanche, la clause de réversibilité devra définir les principes de cette prestation.

Prévoir des dispositions particulières en cas de non respect de l'engagement ci-dessus.

Les principes à définir concernent essentiellement :

- Le délai de mise en œuvre de la réversibilité.
- L'obligation du prestataire de fournir les informations nécessaires à la réversibilité.
- Les conditions de prise en charge de son coût, « a priori » par le client, le cas échéant, sauf faute du prestataire ayant conduit à une rupture anticipée du contrat. Dans ce cas, ce dernier pourra se voir imputer tout ou partie de cette charge.
- Le format de transfert des fichiers et données (format « standard » du marché au jour de la réversibilité et/ou compatible avec le format utilisé par le client à cette date), principe et conditions du transfert au client des logiciels/matériels dont serait titulaire

le prestataire et qui seraient nécessaires à la continuité de l'exploitation, assistance post-migration…

Prévoir la possibilité pour le client de vérifier ou de faire vérifier périodiquement la réalité de l'engagement du prestataire (par exemple la mise à jour du plan de réversibilité).

II.26 - Responsabilité

- Conformément aux règles de droit commun (article 1147 du Code civil) et sauf dispositions contraires, le prestataire est responsable de tout préjudice pouvant résulter d'un manquement de ce dernier à ses obligations contractuelles ; en application de l'article 1150 du Code civil, le dommage indemnisable est celui prévisible au jour de la signature du contrat.
- La responsabilité du prestataire peut être contractuellement limitée, quant au montant total des dommages indemnisables et/ou quant à la nature de tels dommages (les dommages « indirects » sont souvent exclus à la demande des prestataires : perte de clientèle, préjudice d'image…).

  Commentaire *: Sur la portée d'une clause limitative de responsabilité, voir l'arrêt n° 227 du 13 février 2007 de la Cour de cassation (arrêt « Oracle ») rappelant au visa de l'article 1131 du Code civil qu'un manquement à une obligation essentielle est de nature à faire échec à l'application d'une telle clause.*

II.27 - Assurances

- Prévoir l'obligation du prestataire d'avoir une assurance responsabilité civile professionnelle (le cas échéant, stipuler le niveau minimal exigé de couverture : franchises éventuelles, plafond, par sinistre, par année) pendant la durée du contrat.
- Obligation du prestataire de payer à bonne date les primes d'assurances ou cotisations et d'en justifier périodiquement au client ou à sa première demande.

II.28 - Confidentialité

- Définir les documents concernés par la confidentialité.
- Préciser les règles découlant de la classification des informations établie par le client.
- Définir la durée des clauses de confidentialités (duré du contrat plus x années après son terme).
- Pour les informations nominatives, selon disposition de la C.N.I.L. (annexe III jointe).
- Le cas échéant, obligation du prestataire de faire signer un engagement de confidentialité par les personnels et les sous-traitants impliqués dans la prestation.

II.29 - Respect de la réglementation sociale

L'infogérance est une prestation de service informatique du prestataire au bénéfice de son client. Cela étant, dans la mesure où le service informatique en question était réalisé

auparavant en tout ou en partie par le client, l'infogérance est susceptible d'entraîner un transfert des contrats de travail du client vers le prestataire pour ceux des salariés concernés par cette activité, sous réserve des précisions qui suivent.

Il résulte des dispositions de l'article L.1224-1 (anciennement L.122-12) du code du travail qui dispose que : « Lorsque survient une modification dans la situation juridique de l'employeur, notamment par succession, vente, fusion, transformation du fonds, mise en société de l'entreprise, tous les contrats de travail en cours au jour de la modification subsistent entre le nouvel employeur et le personnel de l'entreprise. »

Cette règle est complétée par l'article L. 1224-2 du code du travail qui a inscrit la règle du transfert des créances salariales au nouvel employeur, en application de la Directive communautaire du 14 février 1977.

La règle du transfert des contrats de travail s'applique uniquement si l'infogérance entraîne :

- Le transfert d'une entité économique ;
- Ayant conservé son identité ;
- Et dont l'activité a été poursuivie ou reprise.

L'activité doit être spécifique et bénéficier de moyens propres ainsi que d'une réelle autonomie, tant au regard de ses moyens en personnel que de son organisation et de ses moyens d'exploitation. L'existence d'un personnel propre spécialement affecté à l'exploitation de l'entité transférée constitue une condition nécessaire. Cette condition est remplie en particulier lorsque les salariés disposent d'une qualification particulière.

L'existence d'une entité économique exige également des moyens corporels ou incorporels. Le transfert ne suppose pas nécessairement un transfert de propriété des actifs ; la simple mise à disposition au nouvel exploitant des éléments d'actifs nécessaires au fonctionnement de l'activité est suffisante.

Les juges apprécient les conditions d'application de l'article L. 1224-1 du Code du travail au cas par cas, en recherchant le plus souvent l'intérêt des salariés. Le transfert éventuel des salariés dépend également en pratique de la négociation avec les partenaires sociaux, selon qu'ils considèrent que l'intérêt des salariés est, ou non, d'être transférés (notamment en fonction des avantages procurés ou non par le nouvel employeur).

Au-delà des conséquences, exposées ci-dessus, que peut entraîner la conclusion d'un contrat d'infogérance, il y a bien entendu lieu de rappeler que le prestataire s'engage à respecter les autres règles du droit du travail étant applicable à ses salariés (déclarations sociales et fiscales, travail dissimulé...).

Enfin, un contrat d'infogérance ne doit pas dissimuler des conventions prohibées telles que par exemple le prêt de main d'œuvre illicite ou le délit de marchandage.

II.30 - Non débauchage

- Interdire pour chaque partie la faculté d'embaucher le personnel de l'autre partie pendant la durée du contrat et une certaine période (généralement 1 ou 2 ans) après son expiration.
- Prévoir également la durée de cet engagement ainsi que le montant de dédommagement en cas de non-respect (généralement 1 ou 2 ans de salaires du personnel débauché).

II.31 - Transfert du contrat

Faculté ou interdiction (sauf le cas échéant intra groupe) de transférer le contrat à un tiers ; le cas échéant, solidarité du transférant à l'égard du cocontractant.

II.32 - Intégralité du contrat

Prévoir la caducité de tout acte, accord, convention entre les parties (relatifs à l'objet du contrat) dont la conclusion serait antérieure à la signature du contrat.

II.33 - Notifications

Préciser pour chaque partie l'adresse de notification de toute communication ou mise en demeure de la part de l'autre partie.

II.34 - Droit applicable et attribution de compétence

- Droit applicable au contrat.
- Attribution de compétence aux juridictions judiciaires ou à un tribunal arbitral à désigner (mode de constitution, règles de procédure).
- Il est possible de stipuler, avant la phase judiciaire, une procédure de règlement amiable (prévoir impérativement la durée maximale de cette procédure).

III - L'évolution des risques liés à l'infogérance

Note préalable :

Ce chapitre présente une vision globale des risques liés aux systèmes d'information ainsi que ceux qui apparaissent du fait de l'externalisation. Même si cela n'a pas été évoqué dans ce document, l'infogérance permet aussi de réduire certains risques ou d'améliorer leurs traitements.

III.1 - Les risques chez le client

Le risque dans ce document représente un évènement non prévu qui a une conséquence financière pour l'entreprise.

Notre propos sera d'analyser les conséquences de la mise en place d'une solution d'infogérance sur ces risques afin d'évaluer s'il y a aggravation ou réduction.

III.1.1 - Catégorisation des risques chez le client

Pour analyser les conséquences de l'externalisation au niveau des risques, il convient de classer arbitrairement les risques liés aux systèmes d'information en trois catégories :

1. Les risques juridiques liés à l'utilisation d'un système d'information
2. Les risques liés à la diffusion de l'information
3. Les risques de pertes pour le client

Par ailleurs, les risques non liés aux systèmes d'information mais ayant pour origine l'infogérance / l'externalisation seront évoqués.

III.1.1.A - Les risques juridiques liés à l'utilisation d'un système d'information

Les risques juridiques représentent les risques qui conduisent à la mise en cause de la responsabilité civile ou pénale du client par un tiers (un client, une autorité administrative ou judiciaire, etc.). Cette mise en cause de la responsabilité peut avoir pour origine un acte du client lui-même ou de l'un de ses salariés.

a) Typologie des risques juridiques liés à l'utilisation d'un système d'information.

Les risques juridiques du fait de l'entreprise

La liste ci-dessous est non exhaustive.

- Respect des obligations contractuelles
  Un dysfonctionnement du système d'information est susceptible d'empêcher une entreprise de délivrer ses services ou produits (une entreprise de logistique par

exemple) : ce dysfonctionnement, qui peut avoir pour origine une faute de l'infogérant, risque d'entrainer des pénalités de retard pour l'entreprise. En outre, la responsabilité de l'entreprise peut être mise en cause pour non respect des obligations contractuelles.

- Respect de la propriété intellectuelle
  L'entreprise se doit de respecter les droits de propriété intellectuelle des tiers (droit des marques, droit d'auteur, etc.). Il est possible que des parties du système d'information (gérées ou non par l'infogérant) ou des informations contenues sur le système d'information contrefassent les œuvres ou les titres appartenant à un tiers. Dans ce cas, la responsabilité des deux parties peut être engagée.
- Respect des droits des salariés
- Il s'agit des risques relatifs à la cybersurveillance des salariés, des problématiques liées au secret des correspondances et à la licéité de la preuve d'une faute en cas de licenciement par exemple.
- Respect de la vie privée
  La collecte et l'utilisation de données personnelles sont encadrées par la loi « informatique et libertés » du 6 janvier 1978. La CNIL est le gardien du respect de ces dispositions. Il existe un risque de mise en cause du client en cas de non respect de cette disposition lorsque des données personnelles circulent sur le système d'information.
  Par ailleurs, la diffusion d'informations sur le système d'information est susceptible de causer un préjudice à un tiers : respect de la vie privée, droit à l'image (salariés et tiers qui agissent sur Intranet).
- Respect de l'ordre public et des mineurs
  Dans le cadre de l'exécution de ses activités, le client doit respecter l'intégrité / la dignité humaine, mais également protéger les mineurs. La responsabilité du client peut être mise en cause en cas de consultations de publication de sites Internet illicites par exemple.
- Obligation de loyauté
  Lorsque le client est une société commerciale, elle doit respecter les règles encadrant la vie des affaires : dispositions relatives aux publicités comparatives, droit de la concurrence. Elle doit également s'abstenir de certaines pratiques : publicité mensongère, pratiques déloyales sur le web, *Cybersquatting*, concurrence déloyale, parasitisme.

<u>Les risques juridiques du fait des salariés</u>

- Problématique des blogs, forums, réseaux sociaux, etc.
  L'entreprise est responsable des contenus accessibles sur un blog créé par un salarié de l'entreprise sur son lieu de travail.
- Utilisation abusive des systèmes d'information
  Lorsqu'un salarié utilise le système d'information du client à des fins non professionnelles de façon abusive, l'entreprise pourrait subir des pertes financières.
- Respect de l'ordre public et des mineurs
  Dans le prolongement des considérations ci-dessus, les salariés doivent respecter

l'intégrité, la dignité humaine et s'abstenir de consulter des sites illicites depuis leur lieu de travail.

b) L'impact des risques juridiques

Dans les deux cas mentionnés ci-dessus, le client peut devoir indemniser un tiers en réparation de son préjudice. Le montant de ce préjudice pouvant être fixé par une autorité judiciaire, une autorité administrative ou par une transaction avec le tiers concerné.

Parallèlement à ce préjudice, le client doit prendre en compte les frais qu'il aura engagés pour se défendre. Avec la judiciarisation de la société, ces frais peuvent atteindre des montants importants, voire supérieurs au montant du préjudice indemnisé.

III.1.1.B - Les risques liés à la diffusion de l'information

Au cours de cette analyse, les risques ont pour origine les informations concernant l'entreprise et qui peuvent être amenées à circuler sur des réseaux, aussi bien à l'intérieur qu'à l'extérieur de l'entreprise. Ces informations peuvent être, par nature, très variées :

- Documents stratégiques
- Documents commerciaux
- Accords commerciaux
- Offres commerciales
- Contrats
- Informations sensibles et/ou confidentielles
- Informations comptables.

Il s'agit, en référence au chapitre précédent, d'une atteinte dont l'entreprise est victime. On y trouve les atteintes à l'image et la fuite d'informations commerciales et/ou techniques (savoir faire).

Cette typologie de risque ne sera pas développée, le lecteur pouvant se référer au document "MAITRISE ET PROTECTION DE L'INFORMATION" publié en 2006 par le CLUSIF.

a) Typologie des risques liés à la diffusion de l'information :

Ces risques sont ceux causés par l'utilisation, à des fins malveillantes, de l'information qui circule :

- Perte de confidentialité
- Désinformation
- Rumeur, dénigrement, atteinte à l'image, à la réputation.

Ces risques évoluent du fait de l'externalisation, un tiers pouvant avoir accès à des informations sensibles pour l'entreprise. La maîtrise de ces informations serait impactée du fait de l'externalisation des opérations et d'une méconnaissance de leur classification ou des règles en découlant..

b) L'impact des risques liés à la diffusion de l'information

Les impacts peuvent être de nature très variées :

- Pertes de marchés
- Echecs de négociation
- Pertes de réputation
- Baisse de cours de bourse

III.1.1.C - Les risques de pertes pour l'entreprise (le client)

Sous cette terminologie vont se retrouver les risques qui ont un impact sur les actifs de l'entreprise ou sur son activité.

a) Typologie des risques de pertes pour l'entreprise

Ces évènements peuvent se classer dans deux catégories :

- **Risques physiques**
  Ce sont les évènements qui mènent à une destruction physique des éléments des systèmes d'information tels que :
  - Incendie, explosion, fumées,
  - Dommages électriques, foudre,
  - Tempêtes, dégâts des eaux, évènements naturels,
  - Bris de machine, vol
- **Risques logiques**
  Ce sont les évènements qui vont atteindre les données ou les flux de données sans impacter les équipements informatiques :
  - Malveillance d'origine interne ou externe
  - Virus
  - Erreur humaine
  - Erreur de programmation
  - Accidents (microcoupures, interférences, surtension,...)
  - Interruption de l'alimentation en ressources extérieures (communication, énergie,...)

b) L'impact des risques de pertes pour l'entreprise

Cette indisponibilité du système d'information peut causer une perte financière à l'entreprise. Les typologies de pertes financières suivantes seront utilisées pour identifier les impacts :

- Coûts de remplacement ou de réparation des équipements informatiques
- Coûts de reconstitution des données détruites ou altérées
- Frais de secours

- Frais engagés pour permettre la continuation de l'activité
- Frais engagés pour identifier le problème
- Pertes de chiffre d'affaires
- Détournements de fonds

III.1.2 - Impact de l'externalisation sur les risques (chez le client)

L'externalisation d'un système d'information (partielle ou totale) peut modifier les risques. En effet, la maîtrise du système étant – pour une grande part - passée dans les mains d'un prestataire, mais ce n'est pas systématique.

L'externalisation ne modifie pas nécessairement l'impact de ces risques.

Le contenu et la force du contrat commercial passé avec le prestataire doit pouvoir définir de façon précise quelles sont les mesures à prendre par le prestataire au niveau de la prévention et de la protection. Ce contrat peut aussi être amené à préciser quelles seront les conséquences financières pour le prestataire en cas de non respect des spécifications liées à la sécurité.

Concernant la sécurité, il est important pour l'entreprise de porter un regard critique sur les mesures prises par le prestataire au niveau de la prévention et de la protection afin de les renforcer si nécessaire. En effet, seule l'entreprise peut être capable de juger et de déterminer quel est le niveau de protection attendu en fonction de ses propres contraintes.

L'entreprise restera malgré tout seule face à la réalisation du risque. Il est donc conseillé de faire réaliser régulièrement des audits de sécurité chez le prestataire (cf. § II.24).

III.1.2.A - Les risques juridiques

L'externalisation a un impact sur les risques juridiques dans la mesure où la responsabilité du client peut être mise en cause du fait des agissements de l'infogérant, en cas de non respect de la législation par exemple. Ce sera notamment le cas pour les infractions à la législation du travail (le travail clandestin non déclaré).

A noter que les responsabilités pourraient être partagées par la décision d'un juge, d'un arbitre ou par accord entre les parties. Le partage des responsabilités peut être défini au moment de la mise en place du contrat d'infogérance.

Le contrat doit prévoir, autant que possible, la limitation de la mise en cause du client du fait des agissements illégaux de l'infogérant. En cas d'impossibilité, le contrat doit prévoir les moyens de contrôles dont disposera le client.

Par ailleurs, le client doit conserver ses recours juridiques contre l'infogérant.

III.1.2.B - Les risques liés à la diffusion de l'information

Pour ces risques, les conséquences resteront toujours supportées par l'entreprise qui devra les assumer seule.

Si l'entreprise peut démontrer une faute commise par le prestataire, elle pourra alors l'appeler en responsabilité pour obtenir une indemnisation du préjudice subi. Mais il restera nécessaire de pouvoir évaluer ce préjudice, tâche peu aisée notamment lorsque le préjudice concerne la

réputation, la notoriété, l'image ou en raison de son incidence sur le cours de bourse. De même les notions de "perte de chance" resteront très difficilement évaluables.

Pour obtenir réparation, l'entreprise doit pouvoir démontrer :

- La faute ou l'acte volontaire commis par le prestataire
- Le préjudice subi par l'entreprise
- Le lien entre la faute et le préjudice.

Sauf dans le cas de l'acte volontaire (qui se traitera probablement au tribunal pénal) le montant de l'indemnisation risque d'être limité à la somme fixée dans le contrat de prestation ce qui peut s'avérer notoirement insuffisant au regard du préjudice.

En tout état de cause, il faut aussi prendre en compte que le traitement d'une réclamation, qu'il soit judiciaire ou amiable, prend un certain délai dont seule l'entreprise en supportera les conséquences.

En pratique, ce type de situation se règle souvent par transaction entre les parties avec ou sans arbitrage.

III.1.2.C - Les risques de pertes pour l'entreprise (le client)

Lorsque le système d'information sera indisponible, quelle qu'en soit la cause, c'est l'entreprise qui devra faire fonctionner ses équipements de production, assurer la logistique d'approvisionnement et de distribution, gérer les facturations de ses clients, continuer de fournir ses produits finis en quantité, qualité et délais conformes aux attentes.

Note : l'entreprise (le client) doit toujours pouvoir contrôler l'efficacité de son centre de secours (back-up).

Comme pour les risques informationnels, si l'entreprise peut démontrer une faute commise par le prestataire, elle pourra alors l'appeler en responsabilité pour obtenir une indemnisation du préjudice subi.

Pour obtenir réparation, l'entreprise doit pouvoir démontrer :

- La faute commise par le prestataire
- Le préjudice subi par l'entreprise
- Le lien entre la faute et le préjudice.

Le montant de l'indemnisation risque d'être limité à la somme fixée dans le contrat de prestation ce qui peut s'avérer notoirement insuffisant au regard du préjudice.

De plus, si le prestataire (l'infogérant) peut invoquer des cas de « force majeure », il pourra alors s'exonérer de sa responsabilité. En tout état de cause, il faut aussi prendre en compte le fait qu'un certain délai est nécessaire pour le traitement d'une réclamation, qu'elle soit judiciaire ou amiable, délai dont seule l'entreprise (le client) en supportera les conséquences.

Une nouvelle analyse des risques et l'adaptation du PRA (Plan de Reprise de l'Activité) restent nécessaires.

III.1.2.D - Les nouveaux risques créés par l'infogérance

Le principal objectif d'un infogérant consiste à industrialiser la gestion du système d'information du client. Il en résulte une mutualisation des moyens techniques et humains

avec ceux d'autres clients de l'infogérant. La localisation géographique des prestations d'infogérance peut engendrer de nouveaux risques (risques naturels, géopolitiques, crédits, changes, etc.)

a) L'industrialisation

L'industrialisation de la gestion d'un système d'information (SI), consiste, pour l'essentiel à traduire l'expérience du personnel sous forme de référentiel. Cela permet alors de confier certaines tâches à du personnel moins qualifié ou expérimenté. Pour les traitements simples, cela permet de les faire exécuter à moindre coût, parfois de les accélérer. En revanche, la standardisation fait disparaître la souplesse que l'on trouve souvent dans les équipes informatiques du client (avant le passage à l'infogérance). Lorsque le métier client requiert une très grande vitesse de réaction et d'adaptation, l'équipe de salariés présente certains avantages.

b) La mutualisation des ressources humaines

L'industrialisation amène assez naturellement à la mutualisation des ressources humaines : un individu formé sur une activité technique particulière, peut l'exercer pour plusieurs clients en même temps. Ce que les personnes gagnent en expertise technique, ils le perdent en connaissance du contexte « métier » de chaque client. Cela peut avoir des effets pervers, qui vont à l'encontre de la productivité recherchée.

En outre, pour une équipe mutualisée, la notion d'urgence métier d'un client se limite au respect des SLA, qu'il faut donc définir avec la plus grande attention.

Par ailleurs, il peut exister un risque de « lissage de concurrence ». En effet, l'infogérant peut, afin de rentabiliser légitimement son opération, être tenté de mutualiser le savoir faire propre de son client au profit d'autres entreprises du même secteur d'activité.

c) La mutualisation d'infrastructures

La mutualisation des infrastructures peut revêtir plusieurs formes :

- Partage de locaux : hébergement en centre informatique. Tout évènement dans le « data center » (incendie, inondation…) peut impacter ou atteindre l'activité du client.
- Partage de connectivité : une sortie internet haut débit pour plusieurs clients. Si l'un des clients lance une communication lourde, les autres clients sont impactés.
- Partage de serveurs : hébergement sur un serveur d'applications de plusieurs clients. Si une application consomme trop ou bloque le serveur, les autres clients sont impactés.

Cette industrialisation et mutualisation permettent des gains financiers, mais induisent de nouveaux risques :

- **Divulgation d'informations confidentielles**

  Du fait de la mutualisation des systèmes, il doit être pris en compte le fait que des données sensibles appartenant au client puissent être exposées de manière non intentionnelle à des tiers. Le client perd en effet la maîtrise de ses informations qui circulent sur son système géré par un tiers, l'infogérant.

- **Dommages causés par un tiers**

  Les locaux mutualisés abritent les équipements de plusieurs clients, un dommage pourrait être causé à un équipement du fait du matériel d'un autre client.

  Le premier responsable serait a priori l'hébergeur, néanmoins, il pourrait se retourner contre le propriétaire du bien en cause.

  On constate en général une absence de renonciations à recours entre le Client et l'infogérant ou entre les clients eux même.

- **Risques sociaux liés à la reprise de personnel : le délit de marchandage**

  Le code du travail définit le délit de marchandage comme suit (article L 1221-2 du code du travail) : toute opération à but lucratif de fourniture de main-d'œuvre qui a pour effet de causer un préjudice au salarié qu'elle concerne ou d'éluder l'application des dispositions de la loi, de règlement ou de convention ou accord collectif de travail.

  Ce délit est fondé lorsqu'un salarié de l'infogérant est détaché chez le client et qu'il a un lien de subordination sur le salarié (congé, etc.).

- **Transfert du contrat de travail / Article L1224-1 du code du travail**

  Lorsque survient une modification dans la situation juridique de l'employeur, notamment par succession, vente, fusion, transformation du fonds, mise en société de l'entreprise, tous les contrats de travail en cours au jour de la modification subsistent entre le nouvel employeur et le personnel de l'entreprise.

  Il est essentiel que le client prenne conscience de ce point avant la signature du contrat d'infogérance.

III.2 - Les risques chez l'infogérant

Seules les conséquences chez l'infogérant sont prises en compte dans cette partie.

Les principaux risques sont juridiques et représentent les risques qui conduisent à la mise en cause de la responsabilité civile ou pénale du client par un tiers, du fait des agissements de l'infogérant, de ses salariés, ou ses sous-traitants.

III.2.1 - Les risques du fait de l'infogérant

III.2.1.A - Non-respect du niveau des services attendus

Les niveaux de service que l'infogérant s'engage à fournir à son client dans le cadre d'un contrat d'infogérance sont généralement définis au sein du document appelé SLA *(Service Level Agreement).* Le SLA constitue le cœur du contrat d'infogérance. Les niveaux de service sont fixés en fonction des besoins et attentes du client.

Le non respect par l'infogérant de certains objectifs fixés dans le cadre du SLA est (malheureusement) inéluctable.

Il est donc essentiel de prévoir dans la mesure du possible des sanctions en cas de non respect du SLA par l'infogérant. Ces sanctions prendront classiquement la forme de pénalités contractuelles. Il est nécessaire de les prévoir dans le contrat d'infogérance en précisant le mode de calcul applicable. Ces pénalités devront être proportionnées à l'impact pour le client.

Ces pénalités permettent d'inciter l'infogérant à respecter ses obligations, mais également d'éviter une procédure juridique entre les parties.

III.2.1.B - Non-respect des obligations contractuelles essentielles

Le contrat d'infogérance définit les obligations respectives des parties. Certaines de ces obligations sont essentielles car elles constituent le cœur même de l'objet des prestations de l'infogérant : respect des délais, de la confidentialité, obligation de loyauté, etc.

Il faut noter que les juges ont récemment réaffirmé le fait que l'infogérant ne peut pas s'exonérer de sa responsabilité en cas de non respect d'une obligation essentielle (arrêt Oracle).

III.2.1.C - Non-respect d'informations protégées

Par la nature même de son activité, l'infogérant a techniquement accès à des informations qui peuvent être couvertes par la législation relative à la protection de la vie privée, ou assimilé (droit des salariés, liberté syndicale, etc.).

Le contrat doit prévoir explicitement les modalités d'accès et de manipulation de ces informations à caractère sensible.

À noter que les déclarations à la CNIL restent du ressort du client. Lorsque l'infogérant effectue un traitement non prévu de ces informations, la responsabilité de l'infogérant peut être recherchée.

III.2.1.D - Collaborations avec les représentants de la loi

Par la nature même de son activité, l'infogérant a techniquement accès à des informations du client qui peuvent être requises par les forces de l'ordre ou la justice. Le contrat doit prévoir explicitement l'obligation pour l'infogérant de collaborer avec diligence et dans le respect des dispositions légales, ainsi que les modalités d'indemnisation pour le surcroit de travail généré. Si l'action est due au client, l'infogérant peut refacturer au client. Il serait souhaitable que cette disposition soit prévue dans le contrat par une clause spécifique.

III.2.2 - Les risques juridiques du fait des salariés de l'infogérant

Par la nature même de leurs fonctions, certains salariés de l'infogérant disposent techniquement d'un accès étendu au système d'information (SI) du client. La problématique est identique pour le personnel intérimaire ou les prestataires en régie.

Le contrat doit prévoir, des moyens de contrôle à la disposition du client, lui permettant de contrôler l'activité de ces personnes, et demander sa mise à l'écart immédiate si nécessaire.

Ci-après, deux exemples de motifs sérieux pour justifier celle-ci :

- **Utilisation abusive du SI client**

Certains salariés peuvent détourner à des fins personnelles, généralement à caractère ludique (téléchargement via la liaison Internet du client, stockage de gros fichiers personnels sur les serveurs du client) … Outre la consommation des ressources du client, ces fichiers enfreignent souvent la législation sur les droits d'auteurs, et certains sont pénalement répréhensibles (notamment pornographie impliquant des mineurs).

- **Détournement d'informations du client**

  Certains salariés profitent de leur accès étendu au SI pour collecter des informations confidentielles, dans le but de les diffuser, les vendre ou exercer un chantage quelconque.

Ces risques ne sont pas spécifiques à l'infogérance, mais sont accrus, notamment du fait de la mutualisation des ressources humaines. Les salariés de l'infogérant doivent se conformer à des règlements variés .

III.2.3 - Les risques du fait des sous-traitants de l'infogérant

Le recours à la sous-traitance fait naître des risques similaires à ceux évoqués plus haut, liés cette fois au sous-traitant, ou à ses salariés.

Dans le contrat, il est prudent de prévoir que l'infogérant répond des agissements de ses sous-traitants.

L'appel à la sous-traitance doit être signalé au client uniquement dans le cadre des marchés publics.

L'appel à la sous-traitance ne réduit pas le risque de l'infogérant.

L'impact de ces trois catégories de risques pour l'infogérant sera l'indemnisation qu'il peut être amené à verser à un tiers en réparation de son préjudice. Le montant de ce préjudice pourra être fixé par une autorité judiciaire, une autorité administrative ou par une transaction avec le tiers concerné.

Parallèlement à ce préjudice, le client doit prendre en compte les frais qu'il aura engagés pour se défendre. Avec la judiciarisation de la société, ces frais peuvent atteindre des montants importants, voire supérieurs au montant du préjudice indemnisé.

IV - L'assurance des risques dans le cadre d'un contrat d'infogérance

IV.1 - Rappels sur l'assurance

L'assurance se classe en deux grandes catégories assurance vie et assurance non-vie. Le sujet que nous traitons n'est concerné que par l'assurance non-vie. Au sein de l'assurance non-vie, il y a deux familles :

- L'assurance des biens : le contrat d'assurance indemnisera l'assuré pour les préjudices qu'il a subi.
- L'assurance des responsabilités : le contrat d'assurance indemnisera un tiers pour les préjudices causés par l'assuré.

Dans le cadre d'un contrat d'externalisation, ces deux types d'assurance sont concernés aussi bien pour l'entreprise que pour son prestataire.

L'activation d'un contrat d'assurance se fera lorsqu'un sinistre répondra aux termes et conditions de ce contrat.

Dans un contrat d'assurance dommage, pour obtenir une indemnisation il faudra que l'assuré démontre :

1) Qu'il a subi une perte quantifiable,
2) Que cette perte correspond aux pertes définies dans le contrat,
3) Que cette perte a été causée par un évènement assuré au titre du contrat.

Dans un contrat responsabilité civile, pour obtenir une indemnisation, il faudra démontrer :

1) Qu'un tiers à l'assuré a subi un préjudice,
2) Que ce préjudice a été causé par une faute définie au contrat,
3) Qu'il y a un lien de causalité entre le préjudice et la faute.

IV.2 - L'impact de l'externalisation sur les contrats d'assurance

IV.2.1. L'impact de l'externalisation sur les contrats d'assurance du client

Lorsqu'une entreprise décide d'externaliser tout ou partie de son système d'information, quel que soit le mode opératoire, cette opération aura des conséquences sur le fonctionnement des contrats d'assurances souscrits par l'entreprise.

L'entreprise devra informer ses assureurs de la mise en œuvre d'une solution d'externalisation car ceci entraîne dans la plupart des cas une modification du risque. Le Code des assurances impose aux assurés d'informer leurs assureurs de toute modification de risque. Les contrats concernés sont principalement les contrats d'assurance dommage qui couvrent les biens mobiliers et/ou immobiliers concernés par la solution d'externalisation, mais peuvent éventuellement aussi être les contrats de responsabilité si les processus externalisés ont fait partie des informations collectées par les assureurs pour la mise en place des contrats.

a) Les contrats d'assurance dommage

Le contenu de l'information à destination des assureurs va dépendre des conditions de l'opération d'externalisation : contrats d'assurances dommages (multi-bureaux, tous risques sauf, tous risques informatiques, bris de machine…). Qui est le propriétaire ? Le gardien des biens concernés par l'externalisation ? Qui prend l'assurance à sa charge ?

En outre, l'entreprise devra évaluer la nécessité de modifier ou souscrire de nouveaux contrats du fait de l'externalisation de prestations. Pour cette démarche, il sera nécessaire de prendre en compte :

- La nature même du contrat d'infogérance (externalisation de process, de biens, de ressources….) ;
- Les scénarios de pertes que l'on souhaite voir assurés ;
- Les responsabilités des parties prenantes au contrat d'infogérance.

L'intérêt pour le client de modifier ou de souscrire un contrat d'assurance Dommage

L'externalisation va concerner 5 points :

1) Les biens : le contrat d'infogérance va concerner des biens. Si ces biens sont détruits il faut vérifier qui supportera la charge financière de les remplacer ou de les réparer. L'entité qui supportera cette charge (l'entreprise cliente ou l'infogérant) doit vérifier si ces équipements sont biens déclarés au titre d'un contrat d'assurance (déclaration sur la valeur et la localisation de ces biens).

2) Les frais et les pertes : l'entreprise cliente va devoir engager des frais pour continuer à exercer son activité lorsqu'un sinistre se réalise. Il est possible de considérer que le dysfonctionnement du système infogéré ou l'indisponibilité de ce système sont des sinistres. Ces frais et pertes peuvent être de différentes natures et être plus ou moins liés aux systèmes d'information, par exemple :

   - Les frais de reconstitution des informations détruites ou altérées par le dysfonctionnement. Ces frais peuvent s'avérer élevés si, par exemple, les sauvegardes sont inexploitables.
   - Les frais supplémentaires. Ces frais peuvent couvrir aussi bien des frais dédiés à l'activité informatique (heures supplémentaires des équipes informatiques appelés pour rétablir la situation, frais de fonctionnement d'un centre de *backup*…) que des frais engagés par l'entreprise par exemple pour lui permettre de continuer son activité malgré l'indisponibilité d'une partie des systèmes d'informations (sous-traitance de processus industriels, personnels intérimaires pour suppléer à la logistique,….).
   - Les pertes de chiffre d'affaires : les pertes de l'entreprise peuvent se traduire par une perte de chiffres d'affaire due à un ralentissement de l'activité, ou même un arrêt de l'activité causé par le dysfonctionnement ou l'indisponibilité des systèmes d'informations.

On constate que les frais et pertes listés ci-dessus vont être principalement supportés par l'entreprise cliente. Pour couvrir ces pertes, le client dispose de deux alternatives :

- Exercer un recours contre l'infogérant en mettant en cause sa responsabilité : généralement les responsabilités des infogérants sont fortement limitées dans les contrats à des montants qui n'ont que peu de rapport avec le potentiel de perte chez l'entreprise (puisque souvent exprimés en fonction du coût de la prestation). De plus, la mise en jeu de la responsabilité va entrainer l'obligation de démontrer qu'il y a eu faute, ce qui peut s'avérer difficile.
- Se retourner vers ses propres assureurs si cela a bien été envisagé dès le départ. En effet, lors de la mise en place du processus d'infogérance, les assureurs doivent être informés afin de prévoir dans les contrats d'assurance la couverture des risques chez l'infogérant.

L'avantage majeur de la mise en place d'une telle police d'assurance est la rapidité avec laquelle le client sera indemnisé en cas de dysfonctionnement du système d'information. En effet, il suffit pour le client de démontrer la réalité de la perte ou des surcoûts engagés. Les polices dommages étant de type "Tous risques sauf", ce serait à l'assureur de démontrer éventuellement qu'un sinistre n'est pas garanti.

Un second avantage est qu'il n'est pas nécessaire d'établir une responsabilité quelconque dans l'origine du sinistre.

Les renonciations à recours :

Ce type de clause contractuelle permet de limiter ou de supprimer la possibilité d'une action en responsabilité engagée par le client envers l'infogérant ou inversement.

Ces renonciations à recours peuvent porter sur les dommages matériels (un préposé de l'infogérant endommage, lors d'une intervention, du matériel appartenant à son client), immatériels consécutifs (suite à ce dommage, le client doit engager des frais) ou immatériels non-consécutifs (une application informatique livrée en retard génère une perte de chiffre d'affaires pour le client).

Il faut porter une attention particulière à ce type de clause car les contrats d'assurances dommages comportent généralement des dispositions qui interdisent à l'assuré d'accepter ce type de clause sans en avoir préalablement informé son assureur. Cela signifie que l'assuré peut se retrouver privé d'une indemnisation par son assureur en cas de sinistre. Il est aussi important de noter qu'une clause de limitation de responsabilité est assimilée à une renonciation à recours.

b) Les contrats d'assurance de responsabilité

Dans la plupart des cas, l'externalisation ne modifie pas le risque de responsabilité du client, tout au plus, cela offre à l'assureur une possibilité de recours supplémentaire en cas de mise en cause du client par un tiers.

Néanmoins, l'externalisation peut, dans certaines situations, modifier l'appréciation du risque faite par l'assureur ; tel est le cas lorsque les prestations « objet du contrat d'externalisation » sont essentielles pour le client dans la délivrance de ses services ou produits à ses propres clients.

Par exemple :

1) Une entreprise de logistique qui externalise son système d'information. Si le système d'information ne fonctionne plus, partiellement ou totalement, l'entreprise peut se

retrouver dans l'incapacité de délivrer les marchandises à ses clients et s'expose à la mise en cause de sa responsabilité.

2) Un éditeur de logiciels en mode Web. Cet éditeur de logiciel conçoit et exploite un logiciel en mode SaaS (software as a service). L'hébergement de la plateforme est réalisé par un tiers. Une indisponibilité de la plateforme du fait d'une négligence de l'hébergeur est susceptible de mettre en jeu la responsabilité contractuelle du client.

Par mesure de précaution et comme pour les contrats d'assurance dommages, il convient de prévenir l'assureur de responsabilité civile du changement de risque.

Il sera porté une attention toute particulière aux clauses de renonciation à recours ou aux limitations de responsabilités qui seraient introduites dans le contrat d'externalisation. En effet, ces clauses peuvent avoir un impact sur l'application des garanties responsabilité civile lors de sinistres.

IV.2.2. L'impact de l'externalisation sur les contrats d'assurance de l'infogérant

c) Les contrats d'assurance dommage

Les contrats de dommages permettront de couvrir les équipements de l'infogérant ou ceux du client (dans la mesure où cela est convenu entre les parties et que l'assureur de l'infogérant est informé).

En complément, l'infogérant peut prévoir, au titre de ses propres contrats dommages, de faire couvrir par son assureur les frais qu'il serait amené à engager en cas de sinistre sur ses biens ou sur les biens confiés par le client. L'un des intérêts majeurs de cette couverture est de pouvoir éviter la mise en cause par le client au titre de la responsabilité en augmentant la capacité de réaction de l'infogérant.

d) Les contrats d'assurance RC Professionnelle

Les garanties responsabilité civile professionnelle ont pour objet de couvrir les réclamations de tiers ou de clients contre l'infogérant qui trouvent leurs origines dans une obligation contractuelle ou quasi-contractuelle, et qui découlent d'une faute professionnelle telle qu'une erreur, une omission ou une négligence.

L'assureur en responsabilité civile professionnelle indemnisera à l'infogérant les frais de défense engagés ainsi que les éventuels dommages et intérêts que l'infogérant peut devoir régler suite à une décision d'un juge ou un accord transactionnel.

Les contrats d'externalisation comportent généralement une clause imposant à l'infogérant de souscrire de telles garanties, stipulant un montant de garantie précis. Il est conseillé de demander à l'infogérant de fournir une attestation d'assurance.

Les principales garanties d'une police responsabilité civile professionnelle d'un infogérant sont :

- Garantie des réclamations relatives à un défaut de performance ou un retard dans l'exécution des prestations ;
- Garanties des réclamations relatives à une faute professionnelle, une omission, une négligence, etc. ;

- Garantie des réclamations relatives aux manquements aux obligations de conseil, d'information, etc. ;
- Garantie des réclamations relatives à la propriété intellectuelle (hors brevets) ;
- Garantie des réclamations relatives à la divulgation d'informations confidentielles.

Il est fortement recommandé à l'infogérant de souscrire une telle police d'assurance dans le cadre de son activité professionnelle.

V - Glossaire

Centre d'appel (*Helpdesk*)

C'est une prestation permettant d'assister les utilisateurs internes des services informatiques. Ce centre d'appel est mis à leur disposition, tant sur le plan du matériel que celui du logiciel.

Convention de services *(Service Level Agreement)*

Commentaire *: à distinguer du « Plan d'Assurance Qualité » qui peut inclure un rappel des « bonnes pratiques » du prestataire mais qui en principe ne sont qu'informatives.*

Un SLA est un accord négocié entre deux parties. C'est un contrat liant le client et son fournisseur (à l'origine fournisseur d'accès télécoms). Il contient la description d'un accord commun du niveau de service à fournir ; les services, les priorités, les responsabilités, les garanties etc. Par exemple, il peut indiquer les niveaux de disponibilité, les niveaux de service, les performances, ou tout autre type de services comme la facturation, et même les pénalités en cas de non respect du SLA.

Historiquement, les SLAs ont été utilisés depuis la fin des années 80 par les opérateurs téléphoniques fixes comme une partie du contrat les liant avec les entreprises clientes. Plus récemment les départements informatiques des grandes entreprises ont adoptés l'idée d'utiliser des SLA avec leurs clients (utilisateurs des autres services de l'entreprise) afin de permettre la comparaison entre la qualité de service fourni avec celui promis, permettant d'évaluer l'alternative à une externalisation des services informatiques.

Les spécifications techniques d'un SLA sont habituellement décrites dans un SLS *(Service Level Specification)* ou dans un SLO *(Service Level Objective).*

Un SLS est prévu pour être un guide opérationnel décrivant la mise en place du service, et le SLO est un sous ensemble du SLS contenant les paramètres des services et objectifs à atteindre par le SLS .

Contenu type :

Les SLAs incluent généralement : la définition des services, la mesure des performances, la gestion des problèmes, les obligations et devoirs du client, les garanties, la continuité de service après catastrophe et la fin du contrat.

Source : Wikipedia avec traduction

Événement

À rapprocher du mot « risque »

L'événement constitue l'occurrence d'un ensemble particulier de circonstances.

L'événement peut être certain ou incertain.

L'événement peut être une seule occurrence ou une série d'occurrences.

La probabilité associée à l'événement peut être estimée sur une période de temps donnée.

Source ISO/IEC Guide 73 :2002

Hébergement

L'hébergement, dans le cadre d'un contrat d'infogérance, c'est le transfert de tout ou partie du système informatique, des applicatifs, des serveurs…vers un prestataire spécialisé, auquel on confie également la charge de la gestion.

Impact (du risque)

C'est la conséquence d'un événement qui se réalise ; cela exprime le niveau des conséquences qui en résultent.

Infogérance

L'infogérance est la prise en charge, dans le cadre d'un contrat pluriannuel, de tout ou partie de la gestion d'un système d'information d'un organisme client par un ou plusieurs prestataires informatiques encore appelés fournisseurs. Les prestations décrites sont alors regroupées dans un contrat communément appelé contrat de service qui définit la relation entre le client et le fournisseur.
Dans le contrat, il y a des rôles de maîtrise d'ouvrage, de maîtrise d'œuvre et des niveaux de services attendus. En fonction des catégories d'infogérance, le vocabulaire est étendu : infogérance sur site, infogérance globale, infogérance d'application, hébergement, externalisation, mais dans les documents y compris en Français, ce sont les termes anglo-saxon que l'on retrouve le plus communément employés : *Outsourcing*, *Insourcing*, *Global Sourcing*, *Outsourcing Offshore* (contracté le plus souvent en *Offshore*), *Nearshore*, *Business Process Outsourcing*, etc.

Infogérance applicative

L'infogérance applicative (ou « outsourcing » d'applications) consiste à déléguer la gestion des progiciels intégrés au système, mais elle reste propriétaire de ces programmes.

Voir également « Tierce maintenance applicative »

Infogérance de parc (bureautique)

L'infogérance de parc couvre tout ou partie des fonctions à assurer pour gérer et faire évoluer le parc des postes utilisateurs et les services de support associés (*Helpdesk* ou assistance bureau, équipe de proximité, gestion du parc, dépannage et maintenance, télédistribution…)

Infogérance de production

L'infogérance de production couvre tout ou partie de la plate-forme matérielle et logicielle qui permet au système d'information d'être opérant. On parle en général de :

- Serveurs de messagerie ;
- Serveurs intermédiaires (impression par exemple) ;
- Serveurs d'application critiques ;

- Des réseaux et des structures de téléphonie ;
- Et des systèmes applicatifs opérants sur ces matériels…

Qu'il s'agisse d'architecture grands systèmes ou d'architecture distribuée.

Infogérance d'infrastructure

L'infogérance d'infrastructure concerne principalement les activités de gestion et de supervision du parc informatique. On peut ainsi parler de mise à disposition d'un Responsable Informatique à temps partagé. Son rôle s'articule autour de 4 axes majeurs :

- Prévention, conseil
- Intégration de solutions
- Assistance
- Fourniture de matériels

Source : absylan.com

Infogérance d'infrastructure distribuée (téléphonie, réseaux, moyens périphériques...)

C'est un ensemble de services comme la supervision des serveurs et des données, le pilotage à distance des systèmes, l'hébergement sécurisé, le support aux utilisateurs…

Source : atosorigin.com

Infogérance globale (infrastructure, applicatifs…)

L'infogérance globale représente la composante complète de l'infogérance (le reprise de l'ensemble d'un système d'information), avec la gestion à la fois des infrastructures matérielles et des applications spécifiques (ou issues de progiciels).

Source partielle : Cigref / Syntec informatique

Plan d'assurance qualité

Le plan d'assurance qualité est un document énonçant les pratiques, les moyens et la séquence des activités liées à la qualité spécifiques à un produit, un projet ou un contrat particulier (Extrait de la norme ISO 8402:1994).

Réversibilité

C'est un engagement de la part du prestataire permettant au client de reprendre, sans difficulté technique particulière, directement ou indirectement, les prestations externalisées confiées au prestataire (prestations concernées au moment de la conclusion du contrat et développements futurs).

Tierce maintenance applicative (ou infogérance applicative)

C'est la prise en charge par le prestataire de la maintenance et de l'évolution de tout ou partie du système applicatif. La TMA ne couvre pas l'exploitation du système applicatif qui est assumée dans le cadre de l'infogérance de production.

La TMA de chaînes applicatives vise le même objectif que la maintenance du matériel, à savoir éviter les défauts de fonctionnements, et lorsqu'ils surviennent, remettre en état dans les meilleurs délais ; elle prend en compte aussi les inévitables évolutions liées à la vie des systèmes ainsi qu'aux nouveaux besoins fonctionnels.

La TMA se décompose en 3 principaux domaines : l'assistance applicative, la maintenance curative et la maintenance évolutive.

- L'assistance applicative permet d'apporter un support fonctionnel et technique aux responsables d'applications ainsi qu'aux équipes d'exploitation du client ;
- La maintenance curative est la maintenance de fonctionnement des applications en production ;

La maintenance évolutive : celle-ci comprend l'ensemble des prestations permettant l'ajout, la modification de fonctionnalités du système d'information ainsi que les évolutions réglementaires, elle intègre la maintenance adaptative permettant de prendre en compte les évolutions liées à des changements de versions de système d'exploitation sur les systèmes hébergeant la ou les applications.

VI - Annexe I

LES NORMES

- ISO 9000 de décembre 2000 : Systèmes de Management de qualité - Principes essentiels et vocabulaire.

- ISO 9001 Systèmes de Management de qualité; Exigences.

- AFNOR Z67-801-1 Infogérance Spécifications

- AFNOR Z67-801-2 Infogérance Mise en œuvre des services

- ISO/IEC 27001: (système de gestion de la sécurité de l'information) et ISO/IEC 27002: (code de bonnes pratiques pour la gestion de la sécurité de l'information)

- Charte d'utilisation des systèmes de base de connaissance de l'Association Française de l'Audit et du Conseil Informatique (AFAI)

- Charte Cigref - Syntec informatique (Infogérance et TMA)

VII - Annexe II

CONVENTIONS DE SERVICE (SLA) ET PENALITES

Il est recommandé de prévoir l'application de pénalités en cas de non respect des conventions (SLA). Ce principe est fondamental pour maintenir la « motivation » de l'infogérant sur le long terme.

Les éléments qui permettent de calculer le respect des SLA et le montant des éventuelles pénalités associées doivent faire l'objet d'une attention particulière. Le respect de quelques règles de base permet d'éviter les principaux écueils contractuels.

1. Accès aux données brutes

Le client doit pouvoir, à tout moment, accéder aux données brutes qui servent pour le calcul des indicateurs. En effet, ce calcul des indicateurs (respect des conventions SLA, voire des pénalités) est généralement effectué par l'infogérant lui-même. Lors de la collecte et du traitement de ces données brutes, des erreurs, et parfois même des négligences, peuvent fausser la validité des résultats.

Concrètement, il est très utile de prévoir contractuellement un accès au système de gestion des incidents. Il sera ainsi possible d'en extraire certaines données brutes, afin de procéder à des contrôles par échantillonnage (nouveau calcul des indicateurs et comparaison avec les éléments fournis par l'infogérant).

2. Définition d'indicateurs pertinents

Les données brutes permettent de calculer des indicateurs, qui seront utilisés pour vérifier si les SLA sont respectées.

Lors de la négociation contractuelle, l'infogérant propose des indicateurs standards, mais le client doit absolument les adapter à son propre contexte. Selon le métier de l'entreprise, les indicateurs devront se focaliser notamment sur :

- La disponibilité (logistique,...)
- L'intégrité (santé, …)
- La confidentialité (recherche, …)

Il est possible de programmer des seuils évolutifs dans le temps.

3. Définition de SLA réalistes

La définition de SLA se base sur un ou plusieurs indicateurs. L'infogérant propose généralement des SLA standards, définis en fonction de sa propre capacité de réponse aux incidents, et par rapport au moyens mis en œuvre (généralement proportionnel au tarif des prestations)

Les SLA ont vocation à être respectées : définir des SLA inatteignables serait une source de conflits, pas de progrès.

Le client doit vérifier que les SLA retenus couvrent les volets les plus critiques de son activité, et que les délais sont compatibles avec ses contraintes « métier ».

Les SLA matérialisent la satisfaction client. Si le client est insatisfait alors que les SLA sont respectés, cela signifie que les indicateurs ou les seuils sur lesquels ils se basent, sont inadaptés.

4. Définition de pénalités raisonnables

Les pénalités ont pour vocation à sanctionner le non-respect des SLA, mais plus encore, à inciter à ce que cela ne se reproduise pas.

Certains clients pourront être tentés de définir des pénalités contractuelles exorbitantes. Cette approche a ses limites, car lorsque d'importantes pénalités sont effectivement dues, cela entraine bien souvent des négociations entre les directions de l'infogérant et du client. L'objectif de la direction de l'infogérant, sera avant tout de limiter le montant dû, mais pas nécessairement de remettre en question son organisation.

Des pénalités raisonnables, et plafonnées, sont souvent bien plus efficaces pour obtenir le maintien de la qualité de service. En effet, une pénalité d'un faible montant fera rarement l'objet de négociation, et l'infogérant pourra la répercuter directement sur le budget de l'équipe concernée. Et c'est souvent à ce niveau que les actions « de progrès » sont les plus efficaces.

5. Vérification de cohérence avec des simulations

Il est vivement recommandé de vérifier la cohérence de l'ensemble « événements, indicateurs, SLA pénalités » à l'aide de simulations et d'en contrôler l'adéquation par rapport au contrat du métier.

En effet, il ne faut pas s'arrêter à certains chiffres flatteurs et se méfier des moyennes sur de trop longues périodes ou un trop grand nombre d'items.

Par exemple, pour un parc de 1000 serveurs, chacun étant critique laquelle de ces deux formules protègera le mieux l'activité client ?

a) L'ensemble du parc sur 1 an, doit avoir 99.999 % de disponibilité *(« uptime »)*

b) Chaque serveur, sur 1 semaine, doit avoir 95 % de disponibilité *(« uptime »)*

6. Evolutions contractuelles

Vu la durée moyenne des contrats d'infogérance (plusieurs années), il est utile de prévoir une possibilité d'évolution des conventions SLA et les pénalités associées. Cependant, en cours de contrat, la latitude réelle de négociation est généralement très limitée.

Lorsque cela est possible, il est nettement plus aisé de prévoir ces évolutions dans le contrat initial. Ci-après un exemple simple d'évolutions :

Contrat de service :

- Indicateur : remise en service d'un serveur critique

- Engagement : inférieur à 4 heures ouvrées
- Période de calcul : trimestrielle

Déclenchement des pénalités :

- 1ère année : délai dépassé dans 30% des cas
- Chaque année supplémentaire : seuil abaissé de 5%

Montant de pénalités :

- 3 premiers mois : pas de pénalités (phase d'intégration)
- Reste de la première année : pénalités définies
- Chaque année supplémentaire : pénalités augmentées de +10%

VIII - Annexe III (Source CNIL)

SOUS-TRAITANCE : CLAUSES DE CONFIDENTIALITE

Modèle de clauses de confidentialité pouvant être utilisées en cas de sous-traitance :

Les supports informatiques et documents fournis par la société **X** à la société **Y** restent la propriété de la société **X**.

Les données contenues dans ces supports et documents sont strictement couvertes par le secret professionnel (article 226-13 du code pénal), il en va de même pour toutes les données dont **Y** prend connaissance à l'occasion de l'exécution du présent contrat.

Conformément à l'article 29 de la loi du 6 janvier 1978 relative à l'Informatique, aux Fichiers et aux Libertés, **Y** s'engage à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.

Y s'engage donc à respecter les obligations suivantes et à les faire respecter par son personnel :

- Ne prendre aucune copie des documents et supports d'informations qui lui sont confiés, à l'exception de celles nécessaires à l'exécution de la présente prestation prévue au contrat, l'accord préalable du maître du fichier est nécessaire ;
- Ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées au présent contrat ;
- Ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales ;
- Prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du contrat ;
- Prendre toutes mesures de sécurité, notamment matérielle, pour assurer la conservation et l'intégrité des documents et informations traités pendant la durée du présent contrat ;
- Et en fin de contrat à procéder à la destruction de tous fichiers manuels ou informatisés stockant les informations saisies.

A ce titre, **Y** ne pourra sous-traiter l'exécution des prestations à une autre société, ni procéder à une cession de marché sans l'accord préalable de **X**.

X se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations précitées par **Y**.

En cas de non-respect des dispositions précitées, la responsabilité du titulaire peut également être engagée sur la base des dispositions des articles 226-5 et 226-17 du nouveau code pénal.

X pourra prononcer la résiliation immédiate du contrat, sans indemnité en faveur du titulaire, en cas de violation du secret professionnel ou de non-respect des dispositions précitées.

En cas d'opération de maintenance ou de télémaintenance

Chaque opération de maintenance devra faire l'objet d'un descriptif précisant les dates, la nature des opérations et les noms des intervenants, transmis à **X**.

En cas de télémaintenance permettant l'accès à distance aux fichiers de **X**, **Y** prendra toutes dispositions afin de permettre à **X** d'identifier la provenance de chaque intervention extérieure. A cette fin, **Y** s'engage à obtenir l'accord préalable de **X** avant chaque opération de télémaintenance dont elle prendrait l'initiative.

Des registres seront établis sous les responsabilités respectives de **X** et **Y**, mentionnant les date et nature détaillées des interventions de télémaintenance ainsi que les noms de leurs auteurs.

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11 rue de Mogador
75009 Paris
✆ 01 53 25 08 80
clusif@clusif.asso.fr

Téléchargez les productions du CLUSIF sur

www.clusif.asso.fr