Gérez le risque Fournisseur « as a Service »

LE GUIDE DE SURVIE
qui assurera la transition de vos plans de continuité et de reprise de vos solutions Cloud.

exægis

OCTOBRE 2016

LIVRE BLANC

CONTENU

Faites face à l'obsolescence programmée de vos PRA et PCA

INTRO

L'informatique en nuage ou « Cloud-Computing » bouleverse les pratiques de nos directions informatiques. Les éditeurs acteurs du cloud computing (éditeurs, hébergeurs, intégrateurs) qui bénéficient de cette vague se trouvent partie-prenante de la continuité des opérations de leur client, ou des clients de leurs clients dans le cas des hébergeurs. Ce changement de consommation, entraîne donc des changements d'architecture des systèmes d'information dont la résilience repose désormais dans une chaîne de services encore plus externalisée.

Avec le Cloud, qu'il soit hybride, privé ou public, les frontières se complexifient, transformant opérationnellement les DSI en agrégateurs de services, tout en restant garants de la bonne tenue des engagements de service du système d'information, et garants de la bonne intégration des briques entre elles. Le DSI doit intégrer la disparition fournisseur dans son plan de continuité et de reprise.

Les pratiques de continuité et de reprise s'en trouvent-elles modifiées, transformées ? Les coûts afférents à ces diligences de continuité sont-ils plus importants ? Ce sont là les enjeux auxquels notre livre blanc répond. Entre renfort de pratiques opérationnelles des DSI, acheteurs, responsable de la continuité, directions métiers et contrôle des engagements des opérateurs du Cloud, chacun des acteurs de la chaîne de service est impacté par le changement. Aucun n'est épargné par cette transformation qui s'opère en profondeur, et qui n'est pas anodine sur le plan de continuité.

Christophe POUDRAI
@XopheP

// A propos de l'auteur

Christophe est en charge du déploiement des processus d'audit et de notation des prestataires du numérique chez exaegis. Il développe et maintient les référentiels d'audit à partir de sa propre expérience de responsable Qualité IT et des référentiels ITIL et e-SCM, et CMMi. L'audit de startups fait également partie de ses activités à partir d'un référentiel propre à exaegis.

Nouveaux usages, Nouveaux risques

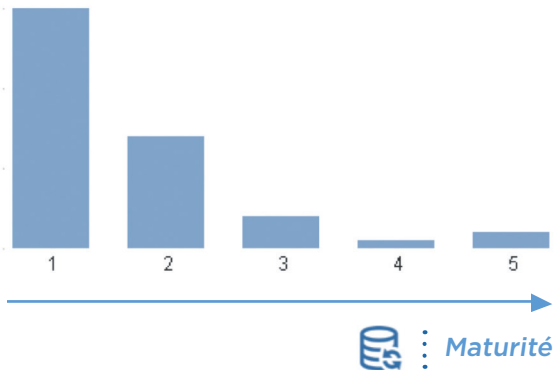
La reprise sur sinistre

Le Cloud, et notamment le SaaS, vont prendre une place de plus en plus importante dans les systèmes d'information, c'est inéluctable ; mais alors quel est l'impact sur nos bonnes pratiques de continuité ?
Le système d'information est désormais multi-opérateurs, il intègre des couches qui dialoguent selon des protocoles certes très standardisés mais dont les acteurs sont multiples. La chaîne de services hébergeurs, éditeurs intégrateurs renforce la complexité du SI et la maîtrise repose désormais sur la capacité à identifier les frontières et à les contrôler (audit, benchmark, surveillance des engagements de service par un tiers).

Les engagements de service de chacun doivent s'empiler correctement dans une orientation pyramidale des services de l'hébergeur à l'utilisateur final. De nouveaux points de contrôle sont à mettre en place pour assurer la continuité. Le PCA, plus que jamais, dépend du PCA des fournisseurs. Les opérateurs Saas ayant simplement « saasifié » leur logiciel sans donner d'orientation « service » à leur offre sont un risque pour le PCA. N'oublions pas que la majorité des entreprises du SaaS sont des PME qui n'ont pas toutes la maturité des services informatiques des grands comptes, rompus eux aux processus IT et aux bonnes pratiques ITIL.

Les résultats de l'étude exaegis sur la base des résultats d'audit menés sur près de 60 éditeurs montre que le PRA est rarement une préoccupation des éditeurs ; en effet, 50% des audités obtiennent une note de 1 / 5 sur le point de contrôle relatif à la mise en place d'un véritable PRA, cela signifie qu'en majorité même si des backups de données sont réalisés, peu nombreux sont les éditeurs qui testent leurs backups, et ont mis en place une procédure de reprise.

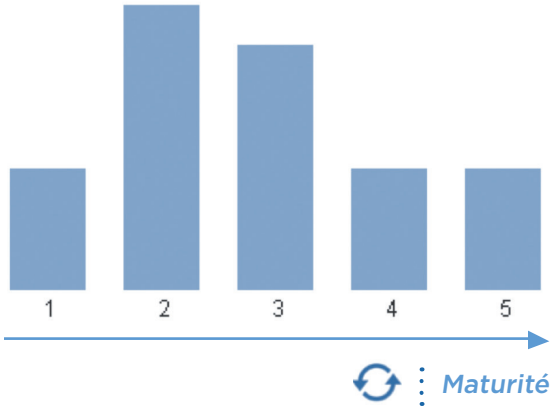
50% des éditeurs réalisent des backups mais n'ont pas de véritable plan de reprise ou se reposent sur l'hébergeur.



Réversibilité

L'usage du Cloud et du Saas n'est pas sans poser des difficultés d'intégration avec les systèmes d'information. Les mesures réalisées par exaegis sont, à l'inverse des résultats sur la présence de plan de reprise, plutôt encourageantes. Les notes obtenues par les audités montrent des capacités de réversibilité hétérogènes et perfectibles (les notes collectées sont en majorité inférieures à la moyenne). Dans 2 cas sur 3, il n'est pas certain que vous soyez face à un éditeur disposant d'API ou de procédures d'extraction automatique de données propices à opérer une réversibilité dans de bonnes conditions.

Des capacités de réversibilité des données hétérogènes et perfectibles.



Dans les deux cas de figure décrits ci-dessous, la réversibilité doit être plus qu'ailleurs passée en revue avant de contractualiser la relation avec le prestataire.

Le ***shadow* IT** : phénomène largement médiatisé, doit passer de l'état de menace à l'état d'opportunité pour l'organisation. Un outil issu du shadow IT largement employé est un outil utile à l'organisation. Il est nécessaire de l'intégrer rapidement, les DSI doivent s'associer à la démarche, au risque de laisser s'installer des bombes à retardement.

L'***innovation, les startups*** : n'ayons pas peur de l'écrire, l'usage de produits innovants présente des risques. Passés les concours internes des grands comptes et d'accompagnement des startups, leurs offres intègrent le SI et deviennent un maillon comme un autre dans la chaîne des services rendus par le SI. Par nature ce maillon est plus faible les premières années où la startup reste en phase de développement et présente une statistique de défaillance élevée.

Et la sécurité ?

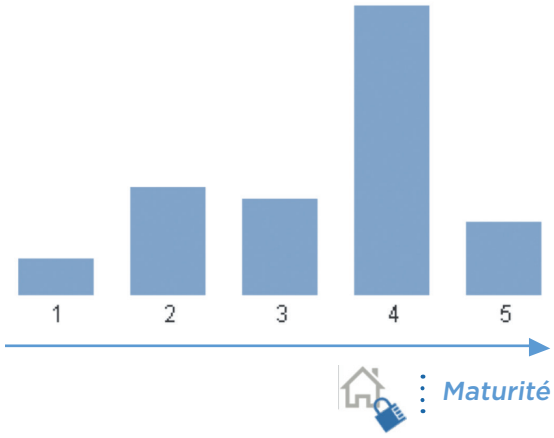
Q : « Cloud is more « secured » ? – A : « It depends ! »

Exægis investigue sur 3 champs « sécurité » que sont : la sécurité physique (les machines sont-elles correctement protégées contre le vol, l'altération physique), l'intrusion système et applicative, et la sécurité des processus.

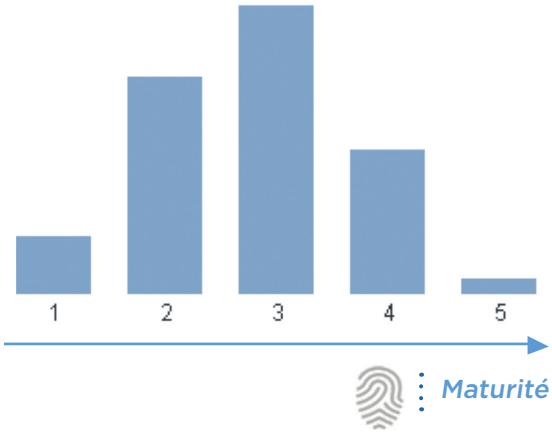
L'émergence des datacenters de haute disponibilité et de haute qualité montre une progression des moyens de sécurité physique. Il est maintenant rare de se trouver face à des hébergements « à la papa ».

A l'inverse, beaucoup de choses sont à faire du côté de la sécurité logique et sur les accès aux données ; exægis observe que trop peu d'éditeurs mettent en place une véritable politique d'accès aux données et de contrôle sur les accès aux données (pas de matrice de droits d'accès, pas de contrôle des access-log). Sur le plan applicatif, peu d'éditeurs mettent en place une véritable charte sécurité prévoyant des tests de sécurité du code et post-déploiement des tests anti-intrusion.

La sécurité physique des serveurs de bonne facture dans la majorité des cas.



La sécurité des accès et du code applicatif encore délaissée.



Les Fondamentaux de la continuité

Les bonnes pratiques de continuité d'activité sont similaires à celles de Risk Management et l'on peut les résumer ainsi : identification des menaces, plan de prévention, et plan de mesure correctif.
La première bonne pratique consiste à « *l'identification des menaces majeures pesant sur les activités les plus critiques* » ; « majeures » parce que leur occurrence représente une perte considérable d'actifs de l'entreprise. Cet exercice d'identification permet de déterminer les moyens à secourir en priorité, les scénarios de fonctionnement en mode dégradé.
Les coûts de mise en œuvre des moyens de secours ne doivent pas excéder les coûts potentiellement engendrés par les effets du risque. Le plan de continuité forme une partie de la gestion de risque de l'entreprise.

« La continuité n'est pas un élément fixe et intemporel, elle doit être alignée sur la stratégie d'entreprise »

La stratégie de continuité repose avant tout sur un exercice d'identification des risques pour l'entreprise qui tire sa justification de la stratégie d'entreprise : c'est un exercice dévolu au top management.
Les questions à résoudre sont les suivantes : quelles sont les priorités métiers (la continuité du « Business as Usual » ou bien l'attaque nécessaire d'un nouveau marché, le développement d'un nouveau produit nécessaire à la relance de l'activité ? Quels sont les moyens opérationnels qui supportent cette stratégie (les outils informatiques ou non, les biens matériels, les hommes qui font vivre l'ensemble, les fournisseurs) ?
Sur chacun de ces moyens quelles sont les menaces (panne, rupture de service, défaillance temporaire ou définitive) ?

Business First !

Le plan de continuité Métier (PCM) forme un outil primordial. Issues de l'analyse de la stratégie et de l'analyse du contexte opérationnel de l'entreprise et de ses processus métier, les activités critiques nécessaires à la continuité telle qu'attendue par la stratégie constituent les activités sur lesquelles le plan de continuité métier va se focaliser. L'inventaire des activités critiques s'accompagne de l'inventaire des ressources qui servent l'activité, qu'elles soient matérielles, informatiques humaines, ou financières. On parlera de Business Impact Analysis (BIA).

Sur chacun de ces composants, les menaces sont identifiées : indisponibilité temporaire de ressources humaines du fait d'une pandémie par exemple, incendie, catastrophes naturelles pour les matériels, la rupture de flux financiers et le manque de trésorerie paralysant les ressources financières.

Ces différentes menaces sont propres à chaque organisation et à ses caractéristiques géographiques, géopolitique, organisationnelles, voire culturelles. La fin de l'exercice devrait de manière pragmatique aboutir à des choses simples du type : l'organisation peut-elle fonctionner sans messagerie pendant 12 jours ? En cas de pandémie, les agents commerciaux doivent pouvoir travailler en télétravail ; le système e-commerce ne peut être défaillant plus de 24h, sans quoi les pertes seraient insupportables ; etc.

Les exigences de continuité métier doivent s'exprimer simplement : « Nous ne pouvons pas nous passer de messagerie interne pendant plus d'une journée »

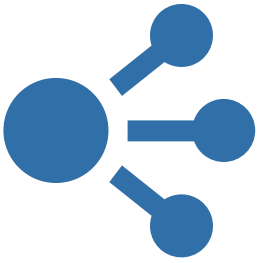
A partir de ces exigences de continuité, l'exercice de calcul du coût de couverture du risque par la mise en place de moyens de prévention ou de contournement du risque peut démarrer. Il intégrera bien sûr des dimensions humaines, organisationnelles, financières.

Etablir l'alignement des moyens IT

Le plan de continuité Métier (PCM) intègre donc les problématiques informatiques par essence, mais compte-tenu de la dimension grandissante du système d'information et de sa place prépondérante dans le dispositif central de l'entreprise, l'exercice de continuité a été spécialisé pour les moyens informatique : on parle alors de Plan de Continuité Informatique (PCI).

L'inventaire des activités critiques et des exigences de continuité d'activité doit naturellement mener vers les moyens informatiques supports à l'exécution de ces activités, et des moyens de continuité propres au système informatique : backups plus ou moins profonds, procédures et tests de restauration, redondance de branches réseau, de firewall, de serveur, de bases de données...

La traçabilité entre les processus de l'entreprise et les moyens informatiques logiciels et matériels permet de mener l'analyse d'impact pour déterminer les éléments logiciels et matériels « à secourir » parce qu'ils entrent dans l'exécution d'un service critique. C'est l'analyse Top-Down. Inversement, la traçabilité devra permettre en cas de défaillance d'un système ou sous-système de connaître l'ensemble des moyens impactés et la conduite à tenir, en terme de communication avec les utilisateurs métier de ces systèmes.



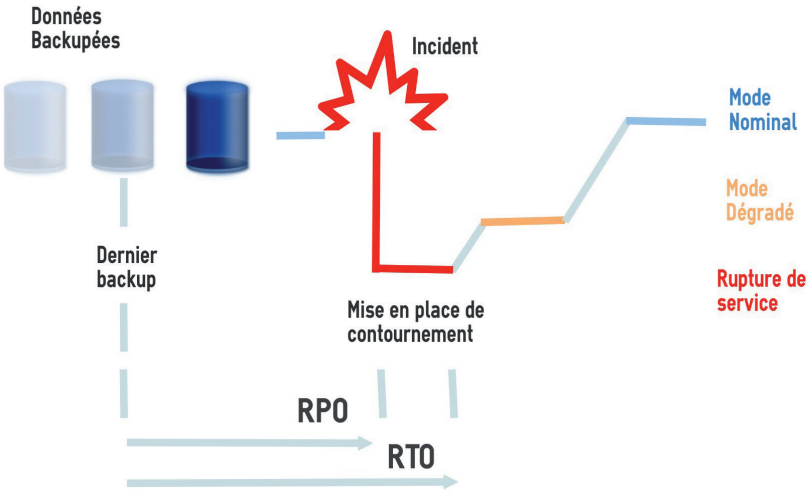
La traçabilité Processus Métier / composants IT incontournable dans l'élaboration du plan de continuité.

L'élaboration du PCI aura donc comme objectif de déterminer les composants applicatifs et matériels critiques et de déterminer les moyens de secours à mettre en place. Ces mécanismes de continuité ont un coût. Il est possible de backuper les données toutes les heures, les nuits, les semaines et le budget à allouer sera différent. L'impact sur le plan de capacité du SI sera là aussi important. Il est donc incontournable de mesurer le coût du Plan de continuité, et s'assurer qu'il n'est pas supérieur aux coûts des risques couverts.

Les Idées fausses !

« Le plan de continuité est l'affaire des informaticiens »

Chaque moyen de continuité IT doit être mis en balance avec les objectifs de Délai d'Indisponibilité Maximal Admissible (DMIA) présents au PCM pour en déduire des délais techniques de rétablissement (*RTO – Recovery Time Objectives*) ; Il en est de même pour les Pertes de Données Maximales Admissibles : en cas de rupture de service, le backup servant à la reprise peut avoir une antériorité plus ou moins importante en fonction des moyens de backup déployés. La perte de données admissible inscrite au PCM est analysée par les services informatiques pour déterminer le RPO – *Recovery Point Objective*, c'est-à-dire la perte de données maximale, et mettre en place les moyens de backup de données ad-hoc.



« Un plan de continuité coûte un bras »

Il se peut également que par manque de traçabilité dans le système d'information, les moyens de continuité mis en œuvre soient surdimensionnés parce qu'alors le reflexe sera de tout backuper et redonder pour être sûr de ne rien oublier (même les choses inutiles). Le processus de gestion de configuration des éléments du SI est donc un élément primordial dans l'élaboration du plan de continuité informatique. Sans gestion de configuration, le backup et la redondance « à tout va » vont accroitre les coûts sans certitude de l'acuité du plan, et de la recherche du juste besoin de redondance. La gestion de configuration et l'analyse de risque de rupture de continuité devront déterminer les matériels et logiciels critiques. On parle de *Single Point Of Failure*, pour lesquels des moyens de prévention des pannes sont nécessaires. La couverture par un plan de reprise de ces éléments devrait mettre le système d'information à l'abri de grosses pannes, ces moyens de prévention passent par une densification du processus de changement de ces éléments critiques, et du processus de mise en service (avec une procédure de retour arrière correctement documentée).

Les erreurs !

« Un PRA mais pas de PCA, et souvent réduit à un PRI (Plan de Reprise Informatique) »

Le plan de reprise d'activité (PRA) couvre les aspects reprise sur sinistre, on parle alors aussi de DRP (Disaster Recovery Plan). C'est une partie du PCA qui adresse les situations de sinistres majeurs : incidents climatiques, incendie, épidémies... La continuité ne se limite pas à ces aspects et bien souvent les entreprises abordent malheureusement la continuité seulement du point de vue de la reprise sur sinistre. Qui plus est le PCA et le PRA sont souvent réduits aux aspects informatiques... Les équipes informatiques sont généralement plus sensibilisées aux problématiques de continuité ; même si bon nombre d'opérations sont informatisées, il n'en reste pas moins que l'humain est encore bien présent dans les opérations. L'identification des ressources humaines opérationnelles critiques et leur « backup » sont tout aussi importants que le backup des données. Les dimensions humaines et processus métier doivent être intégrés dans le PCA, d'autant plus pour les entreprises internationales.

« Pas de tests de PRA »

Les points critiques sont identifiés, les scénarios dégradés sont identifiés et documentés, mais ils ne font pas l'objet de tests à fréquence établie ; imaginons un groupe électrogène qui n'est jamais démarré de manière préventive, des extincteurs qui ne sont testés ni remplacés. Il en est de même pour les plans de continuité. Le VPN prévu pour permettre aux opérateurs de faire du « Home office » en cas de pandémie est-il activable ? Quelle sont les personnes en mesure de l'activer ? L'entreprise doit tester son plan de manière fréquente pour s'assurer que ce dernier a bien fait l'objet de mises à jour en fonction des changements opérés sur les ressources humaines et sur les moyens d'infrastructure. Ne pas faire ces tests, c'est oblitérer le succès du plan de continuité par des oublis ou des approximations.

Encadrer le risque fournisseur Cloud

Certains fournisseurs deviennent critiques parce qu'ils exécutent une partie des processus critiques ou qu'ils fournissent la matière première du processus de production ; ces fournisseurs doivent être profilés, analysés et des solutions de substitution entrevues.

L'assurance qualité fournisseur joue un rôle prépondérant dans la sélection et le suivi des fournisseurs clés. Concernant la continuité, l'analyse de risque métier s'étend sur le domaine de la défaillance financière des fournisseurs clés, et sur le niveau de dépendance avec le fournisseur. A titre d'exemple, engager des actions visant à aider un fournisseur à se développer auprès d'autres clients est une action de prévention des risques de rupture de continuité ; dans le même esprit, le choix d'une startup pour ses caractères innovants doit s'accompagner de mécanismes d'aide au développement pour s'assurer que la startup du jour deviendra le fournisseur fiable de demain.

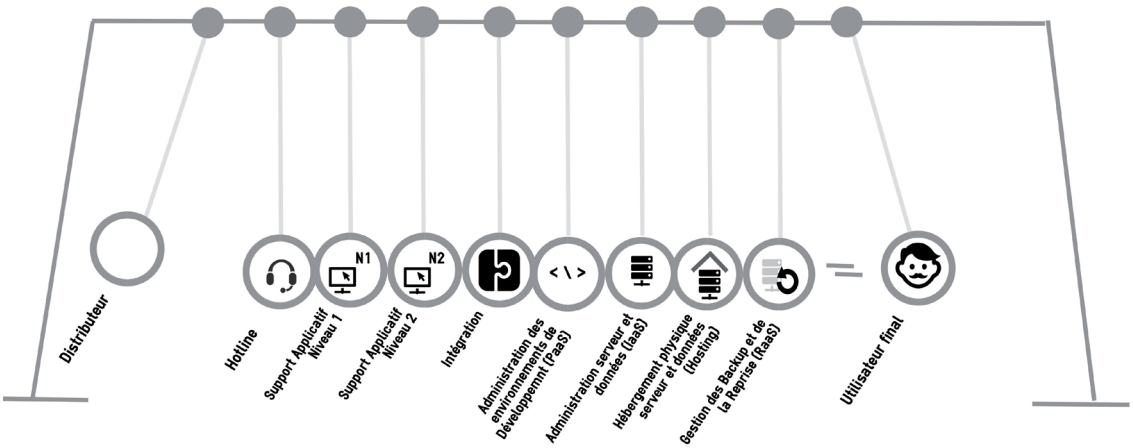
Il y a urgence à renforcer la sélection des fournisseurs ; l'achat ne porte plus uniquement sur une licence « on premise » mais sur un service (hotline, disponibilité, sécurité, temps de réponse…). Connaître les vraies capacités du fournisseur sur ces thématiques et mesurer l'écart entre le côté « slideware » et le côté « opérationnel » devient une nécessité.

L'évolution de la gouvernance achat doit aller vers la formation des acheteurs à cette nouvelle forme d'offre IT, à la mise en place de contrôle, de type Assurance Qualité Fournisseur au même titre qu'un fournisseur entrant dans la production de biens manufacturés. Le PCM doit désormais intégrer les fournisseurs IT !

Le PCI doit faire de même ! Quelle garantie de continuité ? Quels engagements de réversibilité ? La surveillance fournisseurs post achat est elle aussi à renforcer : la défaillance d'un prestataire on-premise n'empêche pas les opérations, la défaillance d'un prestataire SaaS ou Cloud introduit des ruptures d'exploitation : quelles solutions de secours ?

Identifier la chaîne de services

Beaucoup d'utilisateurs du Cloud ou du Saas ne se doutent pas de la chaîne de services qui sous-tend l'usage de leurs applications. L'exemple le plus parlant est l'achat de solutions bureautiques qui peuvent intégrer des fonctionnalités de copieurs, fax, fax-to-mail, GED, outil de dématérialisation… ; ils sont face à des distributeurs qui présentent une offre intégrée mais dont les acteurs entrant dans la chaîne de maintien en condition opérationnelle peuvent être multiples. Cette multiplicité est croissante avec l'usage du Cloud. En première ligne, le revendeur peut déployer des outils logiciels (GED par exemple) qu'il a achetés en marque blanche et dont la tierce maintenance applicative est réalisée par un tiers qui assurera le niveau 2 de support. Cette solution peut être hébergée chez le revendeur qui aura loué des m² dans un datacenter ou bien des serveurs mutualisés, ou encore chez l'éditeur de la solution en marque blanche… Les hypothèses sont multiples et l'on passe sous silence d'autres services pouvant entrer dans la chaîne de services : présence d'intégrateurs ayant développé des modules spécifiques pour le client, solution de backup et de reprise pouvant aussi être externalisée (les solutions RaaS « Recovery as a Service » en premier lieu).



Seul recours, l'audit de la chaîne contractuelle, la vérification du bon alignement des engagements de service dans une vision pyramidale, de la bonne adéquation des moyens de chacun avec les engagements, et la surveillance continue de la pérennité financière de chaque maillon.

Sécuriser les maillons faibles

La défaillance d'un ou plusieurs acteurs de la chaîne de services doit faire l'objet d'un scénario du Plan de Reprise, que ce soit parce que le service peut introduire des ruptures d'exploitation de la société, soit parce que les données exploitées au travers du service sont sensibles et présentent des risques importants d'image en cas de pertes ou de fuites (cas des données RH, données financières, portefeuille client CRM).

De la même manière que la protection d'un applicatif peut être faite au travers d'un mécanisme de « Software Escrow » ou séquestration de code de manière à pallier la défaillance d'un éditeur logiciel « On-Premise », il n'y a aucun frein à mettre en place un mécanisme de « Cloud Escrow » de manière à assurer la continuité de service d'une solution SaaS par exemple. Le client Saas acquiert un droit d'usage tout au long du contrat, et doit garder l'accès à ses données quels que soient les événements intervenant sur les acteurs de la chaîne de services.

Après le « software escrow », place au « cloud escrow », la seule manière de rester indépendant des aléas pouvant intervenir sur un fournisseur IT du Cloud (dépôt de bilan, rachat hostile, inexécution de contrat…)

Les moyens à mettre en place sont multiples mais incontournables pour se mettre à l'abri du risque de défaillance fournisseur, ils adressent les domaines juridiques de propriété intellectuelle et les techniques de backup de données et d'architecture :

- Le maintien de la propriété intellectuelle des briques logicielles à travers un mécanisme de séquestration de code.
- Le maintien des moyens de production même en cas de défaillance de l'éditeur lui-même détenteur du contrat d'hébergement.
- La ségrégation des données de l'environnement Saas sur un environnement tiers ou propriétaire du client.
- La synchronisation des données ségrégées à un rythme dépendant du risque pressenti sur l'éditeur et enfin la recherche d'un prestataire de secours qui sera en mesure de reprendre l'exploitation du service en cas défaillance jusqu'au terme du contrat.

CONCLUSION

Ne sous-estimez pas l'impact du passage au Cloud sur votre continuité d'activité.

Il est temps de faire la reconstitution de notre scénario de continuité ; là ou avant nous achetions des licences logicielles à des prestataires qui venaient nous les installer sur notre infrastructure, la continuité était l'affaire du DSI qui à partir d'exigences métier de continuité bâtissait un PCI et un PRI testé annuellement.

Laissons la place aux offres Cloud et à une chaîne de services applicatifs, d'infrastructures hébergées dont le seul moyen de contrôle est le contrat de services ; la continuité repose maintenant sur l'analyse profonde des contrats sur des aspects propres à la continuité, sur la tenue des engagements des divers intervenants externes. Les pratiques d'audit, de tests conjoints de PRA, de mesure de SLA par des tiers de confiance sont autant outils nécessaires à votre continuité d'activité.
Il est temps de resserrer les lignes entre DSI, Achats et Métiers et d'instaurer une gouvernance globale dans les choix de la mise en place de nouveaux services IT, et le suivi de la qualité de service de vos prestataires tout au long de vos contrats Cloud.

Gardez la maitrise de votre PCA, bénéficiez du Cloud en toute sécurité !

Choisir un prestataire exécutant une partie de votre production mérite que vos mécanismes de prise de décision s'appuient sur des critères formels de stabilité, de fiabilité, de sécurité, de continuité de service, et pas uniquement sur des présentations ou des documentations !
Pour bénéficier de ce nouveau mode d'usage des ressources informatiques en mode abonnement, sans prendre de risques de pertes de données, de rupture d'exploitation sans moyens de reprise, exaegis a intégré pour les grands comptes ces éléments dans ses différents services.

Ces services couvrent l'ensemble du cycle de vie de la solution Cloud :

- **Audit et notation** en amont de la relation afin de mieux connaitre la chaîne de service entre les fournisseurs et leurs capacités (Assurance Qualité Fournisseur).
- **Surveillance** des capacités opérationnelles et de la pérennité financière du fournisseur. Mise à jour deux fois par an de la notation.
- **Garantie Opérationnelle** pour s'affranchir des aléas pouvant intervenir sur le fournisseur (assurance d'une continuité de service).

Un mot sur le label TRUXT

Exaegis met à disposition des Grands Comptes le label TRUXT distinguant les acteurs du numérique pour leurs capacités opérationnelles et leur pérénité financière.

À travers le label TRUXT délivré par Exaegis, un prestataire de solutions numériques et technologiques est heureux de pouvoir nourrir la confiance que ses clients ont placé en lui. Ce label est obtenu après la réalisation d'un audit in situ piloté par les auditeurs Exaegis. Il repose en premier lieu sur une analyse financière grâce à laquelle votre prestataire a été noté de A à c afin d'évaluer les risques de défaillance. Les auditeurs Exaegis s'attachent à évaluer son « risque opérationnel » à travers sept chapitres d'analyse et 150 points d'attention :

Les 7 chapitres d'analyse :

1. Commerce et relation client
2. Production des services
3. Ressources humaines
4. Amélioration de la qualité
5. Gestion des menaces récurrentes
6. Transferts de services (intégration et réversibilité)
7. Modèle économique - Pilotage

Cet audit 360° donne une notation, qui rend un prestataire éligible au label TRUXT ou donne à ce dernier les axes de renfort à mettre en place pour obtenir le label. Le label est délivré pour une durée de 3 ans et fait l'objet d'un réexamen à date anniversaire (nouvel audit) et à date de communication des bilans financiers annuels. Exaegis maintient ainsi un contrôle régulier de la santé financière du prestataire et des événements intervenants au sein de l'entreprise pouvant nuire aux opérations de manière à anticiper les défaillances pour le compte de ses clients grands comptes. Le label installe le fournisseur dans une dynamique d'amélioration sur la base d'analyses à partir des référentiels du marché, et permet aux grands comptes d'avoir une information continue de la santé de ses fournisseurs.

EVALUEZ CE CONTENU

Excellent

Bien, mais je manque encore d'informations

Bof, peut mieux faire

Aidez-nous
à nous améliorer

Cliquez ici pour évaluer