LIREC

Lettre d'information sur les Risques et les Crises

N°51 - JUIN 2016

ACTUALITÉ NATIONALE

MANAGEMENT DE CRISE OU CRISE DU MANAGEMENT, et si notre regard changeait ?

ACTUALITÉ EUROPÉENNE

LA SÛRETÉ DANS LES TRANSPORTS FACE AU RISQUE TERRORISTE

CONTINUITÉ D'ACTIVITÉ

LA CONTINUITÉ DES ACTIVITÉS SOUS TRAITÉES

DOSSIER THÉMATIQUE

RÉSEAUX SOCIAUX *et gestion de crise*

INHESJ

CONTINUITÉ D'ACTIVITÉ

LA CONTINUITÉ DES ACTIVITÉS SOUS TRAITÉES

Dans le cadre de la sécurisation de la continuité des activités d'un organisme, se pose le problème de la défaillance des sous-traitants et fournisseurs externes face à un sinistre majeur. En effet, tout incident grave ou durable chez un fournisseur est un risque qui peut entrainer une rupture d'activité pour l'organisme selon la criticité des tâches confiées. Les prestations de fournisseurs externes sensibles peuvent être très diverses, par exemple, la paie, la numérisation de document, le traitement de chèques, un centre d'appels, une sous-traitance de SAV, ou encore un fournisseur de pièces pour l'industrie.

La sécurisation de ces externalisations est très réglementée pour des secteurs tels que les banques, les assurances ou encore la défense nationale.

Dans le secteur de l'assurance, on entend par sous-traitance « un accord, quelle que soit sa forme, conclu entre une entreprise d'assurance ou de réassurance, et un prestataire de services, accord en vertu duquel ce prestataire exécute soit directement, soit en recourant lui-même à la sous-traitance, une procédure , un service ou une activité, qui serait autrement exécuté par l'entreprise d'assurance elle-même » (Directive Européenne Solvabilité 2 article 13-28). A noter que les entreprises d'assurance et de réassurance conservent l'entière responsabilité du respect des obligations qui leur incombent lorsqu'elles sous traitent des fonctions ou activités d'assurance ou de réassurance. De plus, la Directive Solvabilité 2 impose également que cette sous-traitance ne nuise pas à la prestation continue d'un niveau de service.

De même, les établissements de crédit et les entreprises d'investissement sont tenus de respecter vis-à-vis de leurs fournisseurs, dits Prestataires Essentiels Externalisés (PEE), l'arrêté du 3 novembre 2014. Celui-ci prévoit que leurs PEE s'engagent sur un niveau de qualité en fonctionnement normal du service et sur un niveau de secours en cas d'incident, tout en assurant la protection des informations confidentielles confiées, relatives aux clients de la Banque. A défaut, les banques doivent s'assurer que leur propre plan d'urgence et de poursuite d'activité tient compte de l'impossibilité pour le prestataire externe d'assurer la prestation et pouvoir ré-internaliser le processus concerné, s'il concoure à l'activité bancaire.

Le sujet est d'autant plus sensible pour ces secteurs qu'il fait l'objet de contrôles des régulateurs :

- ✓ L'Autorité de contrôle des assurances (ACPR) exige une information préalable avant toute nouvelle externalisation « importante ou critique » ainsi qu'en cas d'évolution importante ultérieure.
- ✓ l'Autorité de Contrôle Prudentiel et de Résolution (ACPR) des Banques et la BCE ont accès au moins annuellement aux informations sur les PEE d'une banque et peuvent la contrôler en la matière.

La sous-traitance se pratique aussi **dans le secteur public** par le transfert de certaines missions de l'Etat au profit de sociétés du secteur privé, pour des raisons principalement budgétaires ou de réduction d'effectifs.

Les organismes en général, quel que soit leur secteur d'activité ou leur taille, doivent donc sécuriser leurs relations avec leurs sous-traitants « importants ou critiques » au travers des contrats/conventions précisant la continuité des activités confiées, mais également le contrôle et le maintien en condition opérationnelle (MCO) dans le temps du PCA fournisseur.

En amont de toute contractualisation, la notion de risques communs entre l'organisme et ses sous-traitants est rarement évaluée alors que l'étude des risques partagés, comme la couverture du PCA en termes de scénarios de risques, pourrait être un des critères de choix du sous-traitant.

LE PCA DANS UN CONTRAT FOURNISSEUR

La Direction des Achats doit solliciter le Responsable PCA avant toute contractualisation. Au-delà de la notion de force majeure, le contrat avec le sous-traitant doit inclure une clause de continuité d'activité à part entière avec des engagements précis de PCA.

Pour s'assurer de la résilience des activités critiques confiées, l'organisme doit exiger contractuellement certains éléments, à savoir:

- ✓ Un responsable PCA identifié et nommé chez le sous-traitant, pour des contacts en cas de crise et idéalement en dehors de toute crise.
- ✓ Un engagement formel de remontée d'alerte en cas de sinistre, de risque ou de probabilité forte de perturbations (ex : grève, ...) afin que le déclenchement du PCA chez le sous-traitant enclenche une communication de crise adaptée vers les bénéficiaires finaux du service. Cet

engagement est d'autant plus important que dans certains cas l'activité s'insère dans un processus complexe. La chaîne de dépendance peut se voir alors rompue avec des impacts considérables sur le produit ou le client final.

- ✓ Le PCA doit répondre à des scenarios qualifiés par leur ampleur géographique et temporelle. Il doit également permettre un engagement de délai de reprise, par nature de prestation, ainsi que la connaissance des sites nominaux et de repli.

- ✓ Une fréquence de maintien en condition opérationnelle au travers de campagnes de mises à jour et la réalisation d'exercices PCA permettent au fournisseur d'apporter la preuve de la validation et surtout de l'efficience de son PCA. La participation de l'organisme aux exercices réalisés par ses fournisseurs, soit en tant qu'observateur, soit en faisant jouer sa propre organisation est importante, afin de tester de bout en bout la pertinence et l'opérationnalité des dispositifs.

- ✓ Une clause d'audit du PCA.

L'ensemble de ces exigences permet d'avoir une assurance raisonnable de l'engagement du sous-traitant dans une démarche de continuité d'activité de qualité afin de sécuriser les activités critiques sous-traitées.

Ces clauses proposées sont très contraignantes pour le sous-traitant et il n'est pas rare qu'elles fassent l'objet d'âpres négociations. Il n'en demeure pas moins qu'en l'absence de sécurisation suffisante, les risques encourus par l'organisme peuvent être considérables. Dans ce contexte, l'avis éclairé du RPCA ne doit pas être négligé.

Si l'organisme souhaite imposer au sous-traitant le respect de la norme ISO 22301 (Système de Management de la Continuité d'Activité), cette exigence de certification peut très bien se limiter aux processus reliant le sous-traitant à l'organisme.

LE CAS PARTICULIER DU SYSTÈME D'INFORMATION

L'externalisation croissante du système d'information vers des fournisseurs externes (prestataires informatiques, fournisseur de solution cloud…) nécessite une cartographie de la résilience globale. Les fournisseurs mettent en général en place des services clé-en-main gérés par des contrats de service dans lesquels il est pris en compte les items décrits ci-dessus. Mais le problème peut se compliquer quand des Directions métiers achètent directement les applications informatiques sans relation avec la Direction informatique et sans analyse de risques.

LE CAS DES SECTEURS D'ACTIVITÉS ET OPÉRATEURS D'IMPORTANCE VITALES (SAIV - OIV)

Dans son décret N 2006-212 relatif à la sécurité des activités d'importance vitale du 23 février 2006, l'État a défini la notion de Secteur d'Activités d'Importance Vitale (SAIV) dont la démarche de mise en œuvre a pour but de faire en sorte que les Opérateurs d'Importance Vitale (OIV) désignés par l'État, protègent leurs sites névralgiques dits Points d'Importance Vitales (PIV).

En complément, ces OIV doivent rédiger un Plan de Sécurité Opérateur (PSO) et soumettre à l'approbation du Préfet de Département géographiquement compétent, et pour chacun de leurs sites PIV concernés, un Plan Particulier de Protection (PPP). Le Préfet, au vu du PPP, met en place un Plan de Protection Externe (PPE). Ce dernier permettra à l'État de prêter son concours à la protection et au fonctionnement du dit site (par exemple, par l'envoi de force de police et la mise à disposition de ressources contingentées) en cas de risques avérés. Dans la deuxième mouture du SAIV, en cours de déclinaison en 2016, l'État demande aux OIV un compte-rendu annuel sur les évolutions des PCA de l'OIV.

RÔLE DE LA CONTINUITÉ DES ACTIVITÉS SOUS TRAITÉES DANS CE CONTEXTE D'IMPORTANCE VITALE

En cas de sinistre ou d'incident majeur pouvant générer la discontinuité de l'activité d'un OIV sur un de ses sites PIV, l'État et le préfet seront particulièrement sensibles à la continuité de ces implantations. Ils s'assureront, en amont et avec précision, de l'opérabilité en permanence des plans de continuité de l'OIV et de ses sous-traitants concourant au maintien de son activité. Ils se pencheront d'autant plus sur les Plan de Continuité des différents niveaux de sous-traitance (sous-traitant du sous-traitant, …).

CONTRÔLE ET MAINTIEN OPÉRATIONNEL DU PCA FOURNISSEUR DANS LE TEMPS

La mise en place d'un suivi annuel permet de s'assurer que le PCA du prestataire évolue et surtout reste opérationnel. Le contrôle des dispositifs techniques de secours du sous-traitant peut faire également l'objet d'un rapport, tout aussi instructif qu'une visite sur place du Responsable PCA.

La meilleure façon de vérifier qu'un dispositif de secours est efficace est de demander des rapports post-incidents et des comptes rendus d'exercices PCA annuels au sous-traitant ou de participer au test avec lui. Si dans la réalité le test conjoint ou sur place se pratique peu, ceux qui le font régulièrement, par exemple avec un ou deux fournisseurs par an, constatent

SUITE P.50…

que cette collaboration facilite une cohésion mutuelle des équipes autant pour les relations courantes, qu'en cas de coup dur.

Le maintien à jour des annuaires de contact en cas d'urgence n'est également pas à négliger.

LA GESTION DES INCIDENTS ET QUELQUES AUTRES QUESTIONS PERTINENTES À SE POSER

- ✓ Malgré le contrat, le prestataire ne communique pas toujours, quand faut-il s'inquiéter ?
- ✓ Connaissez-vous les sous-traitants de vos sous-traitants ? Certaines des prestations confiées sont-elles sensibles et donc ne doivent pas être confiées à nouveau ?
- ✓ Tout le personnel affecté à vos prestations est-il salarié de votre fournisseur ?
- ✓ Etes-vous le principal client de votre fournisseur ? Sinon quel est son client principal et surtout comment gèrera-t-il ses priorités de reprise entre ses clients en cas de sinistre grave ?

Ces questions peuvent aussi être abordées dès le contrat en s'imposant comme des clauses d'information obligatoires. Une simple visite sur place sera là encore instructive.

Enfin, il peut être extrêmement utile d'avoir un fournisseur alternatif pour les prestations les plus critiques ou de les répartir entre plusieurs fournisseurs par zone géographique ou zones de risques et ainsi éviter des conséquences en cascade. Ainsi, une banque pourra avoir plusieurs transporteurs de fonds pour éviter un blocage complet de ses agences et Guichets Automatiques Bancaires en cas de défaut de l'un d'eux.

Parfois la solution du fournisseur alternatif n'existe pas car il détient un savoir-faire unique, donc n'a pas de concurrence. Une vraie stratégie de résilience renforcée devra alors être mise en place, à savoir : augmenter ses stocks tampons, s'assurer de la résilience des équipes du fournisseur, voire racheter le fournisseur s'il est vital à la survie de l'organisme.

Une piste souvent éludée, peut-être la sous-traitance temporaire à un concurrent mais elle pose le problème des secrets de fabrication.

En conclusion, le bon partenariat avec les fournisseurs, sous-traitants, PEE doit impliquer les achats, le Responsable de l'activité confiée, le Responsable PCA, et selon les cas le Responsable sécurité du système d'information. Le PCA doit alors être vécu comme une occasion de connaissance et d'amélioration de la résilience mutuelle des deux parties ■

LES AUTEURS

Cécile WEBER, RPCA Groupe MAIF - Présidente du CCA.
Monique TINAS, RPCA Caisse d'Epargne IDF - Trésorière du CCA.
Éric MILTON, consultant - Administrateur du CCA.
Emmanuel BESLUAU, consultant - Administrateur du CCA.
François TÊTE, consultant - Président d'honneur du CCA.
Nicolas de THORÉ, consultant – Vice-Président du CCA.

LES PROCHAINS ARTICLES DU FEUILLETON « CONTINUITÉ D'ACTIVITÉ » :

✓ la continuité d'activité et la supply chain (chaîne logistique)

✓ la validation du PCA par des exercices

✓ le maintien en condition opérationnelle des PCA

✓ le système de management de la continuité d'activité et la normalisation