ifaci

institut français de l'audit et du contrôle internes

En partenariat avec :

mega

Organisé en collaboration avec :

Arjuna • Baccou Bonneville Consultants • Mica

Actes du colloque

Continuité d'activité, continuité informatique et gestion de crise

Comment maîtriser vos dispositifs ?

mercredi 21 mars 2012

Cercle National des Armées

Sommaire

Introduction de la séance **4**
Philippe MOCQUARD, 4
Délégué Général, IFACI 4

Discours d'ouverture **5**
Firouz MEGUEDAD 5
Présidente de séance 5

Pannes techniques, catastrophes naturelles, accidents industriels, quels sont les points communs à toutes ces situations de crise ? **6**
Charles-Edouard ANFRAY 6
Délégué Gestion de crise du Groupe, Direction de la Sécurité industrielle, Total 6

Continuité d'activité, continuité informatique et gestion de crise : dessiner et comprendre les frontières entre ces trois activités **11**
Serge BACCOU 11
Directeur associé, Baccou Bonneville Consultants 11
Véronique DEMACHY 11
Directrice associée, Mica 11
Catherine PIEDNOEL 11
Directrice associée, Arjuna 11

Auditer son PCA **16**
Julie-Anne PRUVOST 16
Chef de mission audit de performance, Safran 16
Véronique DEMACHY 16
Directrice associée, Mica 16

LE PLAN DE SECOURS INFORMATIQUE **22**

Mettre en œuvre un programme sur la continuité informatique **22**
Fabrice CHATRON 22
Ancien chef de mission de l'I.G., Responsable continuité informatique, Groupe BNP Paribas 22

Auditer son Plan de Secours Informatique et détecter ses vulnérabilités **27**
Serge BACCOU 27
Directeur associé, Baccou Bonneville Consultants 27

PCA ET GESTION DE CRISE **33**

Comment associer les deux démarches complémentaires : création d'un pôle PCA et Gestion de crise au sein d'Aéroports de Paris **33**
Guillaume TIFFREAU 33
Coordinateur dispositif de crise et continuité d'activité Groupe, SMRR-pôle Défense, Crise et Protection, Aéroports de Paris 33

Comment associer les processus lors d'une simulation de crise ? **35**
Catherine PIEDNOEL 35
Directrice associée, Arjuna 35

Gestion de crise et continuité d'activité : retour d'expérience sur la stratégie développée face à une crise géopolitique de grande ampleur **42**
Michel COUTY 42
COO fonctions de BNPP EGYPT lors des événements survenus en 2011, Groupe BNP Paribas 42

Quels sont les risques majeurs à auditer en matière de PCA/PSI et Gestion de crise ? **46**
Table ronde animée par François TABOUROT 46
Executive Vice-President, Mega International 46
Nathalie DROGUE 46
Responsable Audits Internes, Safran 46
Daniel NOUELLE 46
Responsable de l'Audit Informatique, Air France 46
David RIVIERE 46
Responsable de l'Audit des S.I., GDF Suez 46
Christophe SERRANO 46
Global Policies and Work Environment, Orange Business Services 46

Quelle analogie entre la démarche de résilience au niveau national et celle de continuité d'activité des entreprises ? **57**
Yann JOUNOT 57
Préfet, Directeur de la protection et de la sécurité de l'Etat au Secrétariat Général de la Défense et de la Sécurité Nationale 57

Conclusion **61**
Firouz MEGUEDAD 61
Présidente de séance 61

Introduction de la séance

Philippe MOCQUARD,

Délégué Général, IFACI

Mesdames et Messieurs,

Soyez les bienvenus à ce nouveau colloque de l'IFACI. Nous nous intéresserons aujourd'hui à la gestion de crise, à la continuité d'activité, à la continuité informatique ainsi qu'aux différents acteurs et au rôle des auditeurs et des contrôleurs internes dans ces processus.

Ce colloque sera présidé par Madame Firouz MEGUEDAD, qui possède une expérience de 23 ans dans la banque de détail. Depuis 2004, elle a été successivement responsable des risques opérationnels, puis responsable continuité d'activité au sein du groupe Banque Populaire Caisse d'Epargne.

Madame MEGUEDAD, merci d'avoir accepté de présider ce colloque.

Une vidéo sera réalisée au cours de la journée : un film de quelques minutes en synthétisera les moments forts. Il sera mis en ligne sur le site internet de l'IFACI.

Je vous souhaite à tous une très bonne journée.

Discours d'ouverture

Firouz MEGUEDAD
Présidente de séance

Permettez-moi de me présenter : je suis responsable de la continuité d'activité du groupe BPCE (Banque populaire-Caisse d'Epargne). Le groupe BPCE compte une centaine d'établissements, les banques régionales Banques populaires, les Caisses d'Epargne, Natixis et les autres entreprises du groupe. Il intègre 120 000 collaborateurs, 8 000 agences et 37 millions de clients.

Dans un tel contexte, assurer la continuité d'activité constitue pour nous une préoccupation essentielle. Nous sommes attachés à apporter un service de proximité à nos clients en cas de sinistre et, en priorité, à garantir la sécurité de nos collaborateurs.

L'IFACI a choisi de traiter ce sujet pour plusieurs raisons.

Tout d'abord, les crises sont de plus en plus fréquentes et impactantes (Katrina, Fukushima, Costa Concordia, etc.). En 2010, en France, quatre régions ont été impactées par des intempéries violentes et quatre autres par des sinistres.

Ensuite, la gestion de crise est un élément clé dans le traitement de ces sinistres et la prise en charge de leurs conséquences. Une bonne gestion et une bonne coordination de crise sont en effet essentielles dans la résolution des sinistres.

Enfin, la concentration de l'informatique acquiert une grande importance aujourd'hui. Or nous déléguons de plus en plus à des fournisseurs externes le traitement de notre informatique de production. De ce fait, nous sommes de plus en plus exposés à un sinistre qui impacterait ces fournisseurs.

L'objectif de ce colloque est de partager avec vous des retours d'expériences, à la fois sur des situations d'audit, des plans de continuité informatique, des plans de gestion de crise et des crises vécues.

Pannes techniques, catastrophes naturelles, accidents industriels, quels sont les points communs à toutes ces situations de crise ?

Charles-Edouard ANFRAY
Délégué Gestion de crise du Groupe, Direction de la Sécurité industrielle, Total

Je travaille chez Total depuis une dizaine d'années. J'y ai exercé la fonction de responsable de communication de crise. Puis, je me suis rendu au Yémen afin de coordonner les opérations de sûreté du projet Yemen LNG. Depuis trois ans, je suis responsable de la gestion de crise. En 10 ans, j'ai participé à plus de 50 cellules de crise, beaucoup en exercice, et pour quelques-unes, en situation réelle, en particulier l'an dernier pour le Japon et pour la Libye.

I) Définition de la gestion de crise

Avant de commencer, je souhaiterais préciser ce que nous entendons par « gestion de crise ». Cette notion s'inscrit dans un ensemble qui concerne la maîtrise des risques et des crises.

La maîtrise des risques vise à éviter qu'un accident se produise. Or, parfois, il n'est pas possible d'éviter un tel accident. La gestion de crise se concentre donc sur les actions à mener après la survenue d'un tel événement, dans le but de gérer la situation et de redémarrer les activités.

Le point commun à l'ensemble des crises réside dans la grande diversité des scénarios. En effet, il n'existe pas deux crises semblables. La réactivité et la capacité d'adaptation s'avèrent donc primordiales pour réagir de manière adaptée aux situations.

Un paradoxe apparaît ici : la réaction est à chaque fois différente selon le type de crise à gérer, alors que deux domaines doivent, quoi qu'il en soit, être maîtrisés :

- la communication : quels que soient l'environnement et la crise, l'entreprise peut toujours, en dernier ressort, maîtriser sa communication ;
- la gestion de crise elle-même : l'entreprise a toujours le choix des actions à mettre en œuvre (application de plans de continuité et de plans de crise).

Les auditeurs, dont vous faites partie, jouent un rôle essentiel pour vérifier que les dispositifs sont en place, même si paradoxalement, ces derniers ne sont pas toujours applicables « à la lettre » en situation de crise.

II) Diagnostic des crises

Le point commun à l'ensemble des crises tient au fait que leur diagnostic s'avère délicat. Nous recevons, à travers les médias sociaux et internet, une multitude d'informations, parfois contradictoires. Face à ce flot d'informations, nous développons souvent des réactions de stress et de « silo » : les managers et les responsables ont ainsi tendance à considérer la situation au travers du prisme de leur domaine de compétences.

Les conséquences des crises étant multiples, il convient de porter un regard global sur toutes les situations, tout en développant des capacités d'expertise. En effet, bien souvent, les situations que nous rencontrons nécessitent des regards d'experts : expertise métier, finances, ressources humaines, communication ou logistique, par exemple.

J'insiste sur la gestion du stress, qui reste assez méconnue. Certaines sociétés et certains salariés, face aux différentes situations que nous avons rencontrées l'an dernier, ont réagi de manière totalement inappropriée.

III) La nécessité d'innover et d'imaginer des solutions

De toutes les crises que nous avons vécues, aucune ne s'est déroulée exactement comme le plan l'avait prévu. Il a toujours fallu trouver des solutions différentes et innovantes.

Le cas d'école dans ce domaine est la Pandémie de 2009, qui ne s'est pas du tout déroulée comme prévu dans les plans.

En dernier ressort, je recommande de préparer le scénario « le pire ». Ce scénario doit être « joué » en exercice. Si on sait se préparer au pire, on sait faire face à toutes les situations.

IV) Les signes précurseurs des crises

Si la crise ne peut être prévue, il existe des signes précurseurs. Xavier LE PICHON, spécialiste français de géodynamique, précurseur de la tectonique des plaques, affirme que le séisme japonais du 11 mars 2011 n'a pas été prévu, mais qu'il était prévisible. Il signifie par-là que les risques de séisme ont été calculés en fonction des éléments qui avaient été enregistrés par les instruments sur une période de 100 ans seulement.

En revanche, l'historique des événements survenus sur une période de 500 ans n'a pas été pris en compte. Si tel avait été le cas, il serait apparu que cette période avait connu des séismes encore plus graves que ceux mesurés au cours des 100 dernières années. Sous cet angle, le séisme était donc bel et bien prévisible. Je n'affirme pas que les crises puissent être prévues, mais que des accidents surprenants puissent être anticipés.

Dans un autre domaine, la courbe du prix du blé pendant le « Printemps arabe » présente un premier pic correspondant aux émeutes de la faim en 2008. Début 2011, la courbe remonte. Certes, le cours du blé n'explique pas à lui seul le « Printemps arabe ». Toutefois, il est utile de suivre des indicateurs.

Nous devons donc tous suivre des indicateurs, précurseurs des crises d'une manière ou d'une autre. Chacun a son indicateur, pour une compagnie pétrolière, par exemple, je ne devrais pas vous surprendre en disant que l'un des indicateurs peut être le cours du baril de pétrole ou bien le prix du carburant.

Le sujet de mon intervention porte sur les pannes techniques, les catastrophes naturelles et les accidents industriels. Cependant, certains de ces éléments sont des causes d'accidents, alors que d'autres en sont les conséquences. La panne réseau peut survenir à cause d'un simple accident informatique ou électrique, mais elle peut également être la conséquence d'un tremblement de terre, d'un séisme ou d'un incendie.

En soi, une panne réseau ne constitue pas nécessairement une situation de crise, mais la conséquence d'autres événements, qui peut ajouter à la complexité et rendre la crise plus difficile à gérer encore.

V) La dimension psychologique

Cette dimension m'apparaît cruciale. Avec l'expérience, je me suis rendu compte que ce sujet pouvait parfois être sous-évalué. Quelle que soit l'activité d'une entreprise, on se concentre le plus souvent sur les aspects liés au métier, ceux que l'on connaît bien de l'intérieur, en revanche la notion de perception du public en vient à être oubliée.

Certes, l'étude des faits rassure et permet de se rendre compte du caractère limité des conséquences matérielles d'une situation donnée. Toutefois, lors d'une crise, ce n'est pas

seulement la crise en elle-même qui doit être gérée, mais également sa perception. Le public a besoin d'être rassuré.

Nous ne remplissons pas notre rôle si nous ne gérons pas également les inquiétudes des autres collaborateurs, de notre public interne. Sans communication appropriée vis-à-vis des collaborateurs, une gestion de crise n'est pas parfaitement efficace. Dans ce cadre, la dimension psychologique de communication interne et l'exemplarité du management s'avèrent essentielles. Cette dimension apparaît particulièrement importante dans la société moderne, où chacun a peur qu'on lui cache quelque chose.

Lors de l'accident de Fukushima, Total a mis en place une communication interne impressionnante. Tous les jours – et parfois même plusieurs fois par jour -, Total a communiqué, non seulement vis-à-vis de ses collaborateurs au Japon, mais également en direction des autres collaborateurs du Groupe, pour les informer sur la situation en cours.

Dans le cas de Fukushima, notre problème, sous l'angle gestion de crise, n'était pas tant lié à l'accident lui-même qu'à l'inquiétude des expatriés. Le mot « apocalypse », prononcé à cette occasion par un commissaire européen, a en effet eu des impacts sur les collaborateurs situés en Corée et en Chine, qui se sont alors demandé si une évacuation était nécessaire.

Face à une telle situation, il faut appeler le management et les collaborateurs concernés un par un, ou, si possible, organiser des visioconférences, et non envoyer un communiqué ou un mail qui pourrait être pris comme un manque de transparence ou de la « langue de bois ».

VI) Les éléments pouvant faire l'objet d'un audit

L'entreprise peut maîtriser deux aspects :

- la communication ;
- les fondamentaux.

1) La communication interne et externe

J'ai été beaucoup marqué par un accident qui s'est produit il y a quelques années chez Aéroports de Paris. A cette occasion, chacun a pris la parole : les salariés, le préfet de police, le Ministre de l'Intérieur, le Président de la République, le Préfet, l'architecte, les syndicats, etc. Chacun semblait connaître la cause de l'accident.

Les situations de crise sont plus généralement caractérisées par des prises de parole en tous sens. Dans un tel contexte, l'entreprise doit garder son calme. Elle doit désigner un porte-parole unique et délivrer un seul message en interne et un seul message dans le cadre de sa communication externe. Les porte-paroles doivent être entraînés et formés.

La désignation du porte-parole, les messages communiqués et l'éventuelle préparation des messages à l'avance constituent autant d'éléments qui peuvent être audités. Ils montrent que l'entreprise est prête à réagir à une crise.

La communication interne me paraît être un point critique. Traditionnellement, une entreprise partait du principe qu'il lui suffisait de diffuser un communiqué de presse pour régler une affaire. En réalité, la communication doit se poursuivre en interne, sur le long terme.

2) Les fondamentaux de la gestion de crise

Ces dispositifs recouvrent des procédures d'astreinte, de permanence, d'alerte ou de mobilisation. Ils visent à développer un langage commun vis-à-vis des équipes d'intervention. Les Etats-Unis ont développé le *National Incident Management System* (NIMS), dispositif de gestion de crise commun aux entreprises et aux administrations.

En Europe, un tel dispositif n'existe pas. La Communauté Européenne a seulement lancé le projet Crisys. Au-delà, il est important de réaliser des exercices de crise, de se former et d'assurer des retours d'expériences.

Je conclurai en évoquant le rôle majeur des auditeurs face à ces plans. Les professionnels de l'audit et du contrôle internes nous aident à vérifier la bonne mise en place des fondamentaux. Or, ce n'est qu'à cette condition qu'il est possible de régir correctement aux situations de crise rencontrées.

VII) Questions

Jean-Michel BOULDOIRES, Commissariat à l'Energie Atomique

Au CEA, nous sommes naturellement très sensibles à un événement comme celui qui s'est produit à Fukushima. Dans votre exposé, j'ai relevé deux points, qui appellent de ma part davantage des observations que des questions.

Le premier concerne la communication interne. Je note que vous privilégiez la communication directe plutôt que la note ou le mail. Vous avez également indiqué que votre groupe – tout comme le nôtre – emploie essentiellement des ingénieurs, qui veulent tout savoir et tout comprendre. Pour notre part, nous avons adopté une stratégie de communication interne différente de la vôtre : la transmission, à tous les niveaux de l'entreprise (du manager jusqu'au collaborateur), de l'ensemble des communiqués techniques émis par la cellule de crise.

En effet, le public scientifique ne se satisfait pas d'un échange oral, décliné de manager en manager, et qui s'accompagne souvent d'une déperdition d'informations.

Le deuxième point concerne cette fois la communication externe. Je partage tout à fait votre sentiment : il convient d'adresser à la fois un message interne et un message externe. En revanche, vous n'avez pas évoqué la question des médias, qui nous échappe complètement. Il est possible d'émettre un message clair et simple, mais il peut nous échapper.

Comment, dans votre groupe, et compte tenu de votre expérience, avez-vous géré cette difficulté ?

Charles-Edouard ANFRAY

Je suis très heureux qu'une personne du Commissariat à l'Energie Atomique pose une question, car, à l'occasion d'une rencontre avec les équipes de la communication interne du CEA il y a deux mois, nous avons échangé sur nos pratiques de communication. Nous nous sommes aperçus que notre stratégie et notre vision des choses n'étaient pas si éloignées.

Eu égard à votre population, qui est déjà initiée à la problématique, il me semble que votre choix de communication est normal. La communication interne de Total s'adapte à sa propre population. Tout en développant un niveau de détail technique précis, nous avons essayé de le traduire pour une population non initiée.

Quant à la communication externe, je suis d'accord avec vous : les médias nous échappent. Total en a une grande expérience. Il y a quelques années, nous avons connu l'épisode de l'Erika. Entre 1999, date du naufrage, et 2003, les propos de Total sur les marées noires, le transport maritime et la sécurité étaient véritablement inaudibles.

Si les médias nous échappent, ce n'est pas le cas de nos propos. Dans le cas de BP, qui a connu une marée noire dans le Golfe du Mexique en 2010, ce sont quelques mots maladroits prononcés par les porte-parole de l'entreprise qui restent dans l'esprit du public.

Dans une situation de crise, une personne originaire du pays touché constitue le meilleur des porte-parole. C'est en partie pour cette raison que BP a destitué son patron britannique et l'a remplacé par un Américain.

Firouz MEGUEDAD

Merci, Monsieur ANFRAY. Nous reviendrons sur les questions de communication de crise au cours de la journée.

Continuité d'activité, continuité informatique et gestion de crise : dessiner et comprendre les frontières entre ces trois activités

Serge BACCOU
Directeur associé, Baccou Bonneville Consultants

Véronique DEMACHY
Directrice associée, Mica

Catherine PIEDNOEL
Directrice associée, Arjuna

Véronique DEMACHY

Je suis directrice associée du cabinet Mica, expert en continuité des activités. J'ai eu le plaisir de préparer ce colloque pour l'IFACI avec mes deux autres collègues experts, Catherine PIEDNOEL et Serge BACCOU.

Avant d'entrer plus avant dans les débats, il nous a semblé important de définir les frontières entre les trois métiers que sont la continuité d'activité, la continuité informatique et la gestion de crise.

Nous souhaitons également vous faire découvrir les interfaces qui existent entre ces trois métiers, parfois ignorées ou mal appréhendées par les directions. Un de vos rôles d'auditeurs consiste justement à les comprendre, pour ensuite sensibiliser vos directions.

Serge BACCOU

Je suis directeur associé du cabinet Baccou Bonneville Consultants, spécialisé dans la continuité informatique.

Nous disposons dans ce domaine d'un vocabulaire relativement imprécis. Nous utilisons des termes français, anglais, des acronymes et des mots qui désignent des réalités différentes, que ce soit au sein des entreprises ou entre les entreprises.

Bien souvent, lorsque nous sommes en mission dans les entreprises, nous nous apercevons que les personnes ne se comprennent pas. Elles parlent de PRA, de PCA ou de *disaster recovery*, en leur donnant des sens différents. Ainsi, un informaticien pourra considérer le *disaster recovery* comme étant lié à des problématiques informatiques. Pour autant, un *disaster recovery* peut être un tremblement de terre.

Cependant, ce vocabulaire existe : il est inutile de l'ignorer. Nous avons toutefois tenté de le simplifier à l'occasion de ce colloque. Il nous permettra de communiquer ensemble et de nous comprendre lorsque nous aborderons les différentes thématiques de la journée.

Catherine PIEDNOEL

Je suis directrice associée du cabinet Arjuna, qui a été créé en 1993. Nous avons été les premiers à centrer nos interventions sur la gestion de crise, qui constitue le cœur de notre activité. Nous travaillons dans le domaine préventif à hauteur de 70 % (dispositifs, formations, exercices, etc.) et sur l'accompagnement de crises pour 30 %, notamment au travers d'une astreinte que nous assurons 24 heures sur 24 pour certains clients.

I) Présentation des différentes activités de gestion de crise

1. La gestion de crise

Je commencerai par évoquer le processus de « gestion de crise » que nous mettons en place dans les entreprises. La gestion de crise désigne ici une procédure « chapeau », c'est-à-dire une organisation qui permet de gérer tout type d'événement (problème produit, accident industriel, accident de collaborateurs, mise en cause médiatique, etc.).

Ce dispositif permet d'organiser la prise de décision des équipes dirigeantes, l'évaluation du niveau de crise et le pilotage des situations dans toutes leurs composantes : opérationnelles, juridiques, commerciales, RH et communication.

Le dispositif de gestion de crise permet d'organiser le processus de pilotage et de prise de décision, pour tout type d'événement.

Le PCA et le PCI sont deux procédures opérationnelles qui représentent une composante du processus de gestion de crise. Elles permettent de gérer deux événements majeurs : les événements qui impactent l'environnement de travail et les crises informatiques.

1. Le PCA et le PCI

Véronique DEMACHY (PCA)

Le PCA est un dispositif de gestion de crise qui permet de répondre au risque d'inaccessibilité partielle ou totale à l'environnement de travail habituel. Il est mis en œuvre pour des activités critiques. L'environnement de travail peut être le siège social d'une entreprise, un entrepôt, un site de production, etc.

Le plan est composé d'une stratégie de continuité d'activité, de procédures permettant à l'activité de se poursuivre ailleurs, avec des ressources humaines et matérielles préalablement déterminées. Comme tout autre dispositif de gestion de crise, il fait l'objectif d'exercices et de tests.

Serge BACCOU (PCI)

Pour gérer correctement une crise, il convient de prendre en compte une dimension technique. Les crises informatiques peuvent être à l'origine même de la crise, ou en représenter une conséquence. Pour assurer une bonne préparation à ce type de crise, il faut se doter d'un dispositif documenté. Le jour où une crise informatique surgit, il est trop tard pour mettre en place ce dispositif.

2. Caractéristiques de ces dispositifs

Il s'agit de dispositifs coûteux et complexes à mettre en œuvre. Le recours à des experts, spécialistes des différentes disciplines dans vos entreprises, s'avère donc nécessaire. Par exemple, pour assurer une bonne gestion de crise, il est impératif de recourir à des experts dans les domaines de la sécurité, de la qualité, de la communication et de la gestion de crise.

Les *risk managers* interviennent à mi-chemin entre la gestion de crise et la partie PCA. Depuis quelques années, le métier de responsable PCA est apparu peu à peu dans les entreprises. Si certaines entreprises n'ont pas encore mis en place de responsable PCA à plein temps, d'autres ont créé une filière complète dans ce domaine.

Sur la partie informatique, le PCI ou PSI (plan de secours informatique) est piloté par les directions informatiques elles-mêmes.

Vous l'aurez compris : des spécialistes évoluent dans tous les domaines. Toutefois, s'ils travaillent selon un mode « silo », il est très probable que le dispositif ne fonctionnera pas lors

d'une véritable crise. C'est en effet dans les interfaces que se vérifie la communication efficace et rapide entre les acteurs.

Le temps est très important dans ce domaine. Dans une crise, lorsque du temps est perdu, il n'est pas rattrapé, ce qui peut engendrer de nouvelles perturbations et amplifier la crise.

Des ponts doivent donc être créés entre ces trois démarches. Ce processus n'est pas naturel, car chacun est spécialiste d'un sujet et ne connaît pas le champ de compétence de l'autre. Par exemple, s'agissant du domaine informatique, les informaticiens ne sont pas nécessairement des spécialistes de la communication.

Les auditeurs doivent vérifier que ces ponts sont établis. Si tel n'est pas le cas, ils doivent les encourager.

II) Quelques pistes de réflexion pour l'audit du PCA, des PCI et de la gestion de crise

Véronique DEMACHY

Nous souhaitons donner quelques pistes à ceux qui souhaitent démarrer un audit de leur PCA, de leur PCI ou de leur gestion de crise.

De manière prioritaire, il vous faut étudier les livrables, en rassemblant tout type de document intitulé PCA, PCI ou dispositif de gestion de crise en interne. Ainsi, vous vous rendrez peut-être compte que le contenu que vous y trouverez diffère de ce qui vous est exposé pendant cette journée.

Après une première analyse du contenu de ces documents, vous pourrez en apprécier le niveau de maturité. Avant de vous intéresser aux procédures, essayez de repérer les éléments qui s'apparentent à une stratégie de continuité. Les métiers critiques, leur délai maximum d'interruption et la raison de leur détermination (qualification) comme critiques doivent s'y trouver. Ils permettent ensuite de définir les procédures. La stratégie de continuité est préalable à la définition des procédures et à l'implémentation des PCA. Si la stratégie de continuité n'a pas été matérialisée c'est le signe que le PCA n'a pas été construit dans les règles de l'art.

Vous pouvez ensuite analyser les procédures de continuité et leur contenu pour définir votre programme de travail. Celui-ci doit s'appuyer en majeure partie sur la rencontre des différents responsables de projets. Je vous encourage également à rencontrer des opérationnels, pour déterminer leur implication dans la définition de la stratégie de continuité et des procédures.

Par la suite, vous pourrez vous assurer de l'appropriation de la stratégie de continuité et des procédures par les acteurs de l'entreprise. Les opérationnels doivent connaître les procédures pour les faire vivre.

J'attire votre attention sur la sensibilisation et la formation des acteurs impliqués dans la mise en œuvre de ces différents plans. Très souvent, les exercices suivent immédiatement la rédaction des procédures, sans information à travers la communication interne.

L'ensemble du personnel doit être informé des actions qui pourraient être menées en cas de crise. Les personnes les plus impliquées dans ces processus de continuité d'activité doivent également être formées.

Enfin, si le niveau de maturité de votre entreprise le permet, et le plus tôt possible, vous devez porter votre attention sur la transversalité et les interfaces existant entre la continuité des activités, la continuité informatique et la gestion de crise

Si vous n'avez jamais audité l'un de ces trois sujets, nous vous recommandons de les auditer d'abord par thèmes et par silos. Ensuite, vous pourrez vous attacher à examiner les interfaces entre ces métiers, qui ne sont souvent pas perçues, pas comprises ou mal appréhendées par la direction.

III) Deux exemples d'interfaces pour la gestion de crise

1) *Définir une table de correspondance entre les besoins définis par l'informatique et ceux définis par les métiers*

Serge BACCOU

La première des interfaces lie la partie continuité d'activité et la partie continuité informatique. La continuité d'activité vise à permettre aux équipes de travailler, y compris lorsqu'un bâtiment a été détruit ou est rendu indisponible. Le fait de travailler ailleurs suppose de disposer des ressources nécessaires, notamment informatiques.

Toutefois, les acteurs qui élaborent le PCA et ceux qui travaillent à l'informatique ne parlent souvent pas le même langage. Par exemple, ils n'identifient pas les applications par les mêmes dénominations. Les informaticiens peuvent nommer une application par un code projet informatique ou par le nom commercial d'un produit, alors que les acteurs métiers l'appelleront davantage par une logique métier ou par le nom de l'icône qui se trouve sur le poste de travail. Cette situation peut parfois donner lieu à un dialogue de sourds.

Ce problème peut être résolu en élaborant une table de correspondance. Pour cela, il convient de s'assurer que les métiers ont identifié les applications critiques et que l'informatique a trouvé la dénomination qui lui est propre au sein de la direction informatique.

En général, l'informatique approfondit davantage les ressources informatiques que recouvre une application vue par le métier. Un même nom pour le métier peut donc correspondre à 10 applications pour l'informatique.

Dans ce processus, l'auditeur doit vérifier que la table de correspondance existe ou du moins que les parties prenantes se comprennent.

2. La procédure d'alerte

Catherine PIEDNOEL

Je vais à présent me focaliser sur la procédure d'alerte. Il est primordial de détecter et d'anticiper l'arrivée d'une crise. Aujourd'hui, avec les réseaux sociaux, l'information s'accélère. En l'espace de deux ans, la réactivité est devenue fondamentale.

En gestion de crise, nous sortons d'une logique de plan pour entrer dans une logique d'incertitude. on peut distinguer trois type de situation :

- **L'évènement « gris »**
  Sans qu'il mobilise le dispositif de crise, un évènement indésirable survient. A ce stade, il importe de le « déminer », afin qu'il ne dégénère pas en crise. Dans ce sens, il est très important de « précâbler », le plus tôt possible, l'expert informatique, l'expert métier concerné et la communication.

- **L'évènement « gris foncé »**
  Il s'agit d'un évènement à très fort potentiel de crise. L'alerte est vitale dans cette situation. Les acteurs doivent se préparer à la crise et organiser l'ensemble de ses incidences possibles. Ce moment, crucial, peut durer trois heures comme trois semaines.

- **l'événement « noir »**
  Un évènement catastrophique ou très rapidement médiatisé qui impose de réagir immédiatement. Les équipes mobilisées n'évoluent alors pas dans leur environnement naturel.

Il s'agit de s'assurer que la dimension d'alerte et la remontée d'informations du PCI sont bien prises en compte. Nous devons faire face à de fortes réticences. Les informaticiens ne sont pas des communicants. Pire : ils ont même tendance à affirmer que dès lors qu'ils informent les communicants, la crise est déclarée.

Ces problèmes doivent être « déminés » au préalable. Les différents acteurs doivent se connaître et connaître leurs enjeux respectifs : les enjeux techniques, de continuité, d'une part, et les enjeux commerciaux et d'image, d'autre part. Au stade du PCI, l'évaluation des niveaux de gravité doit être déterminée. Il faut faire le lien entre les astreintes techniques, qui existent dans tous les métiers, et les astreintes de direction, qui ont vocation à assurer une réactivité optimale face à la crise.

IV) Questions

Jean-Michel BOULDOIRES, Commissariat à l'Energie Atomique

Le hasard fait que nous venons de réaliser une mission d'audit sur les moyens dont notre organisme s'est doté pour prévenir ou réparer un sinistre majeur qui entraînerait la perte ou l'indisponibilité durable de nos systèmes d'information.

Le système d'information d'entreprise - j'exclus l'informatique métier – représente environ 12 000 applications différentes. La difficulté majeure que nous avons rencontrée consistait à obtenir, de la part tant des informaticiens que des opérationnels, une priorisation des applications à remettre en route en cas de sinistre.

Avez-vous des retours d'expérience ou une recette permettant de gérer des demandes contradictoires ?

Serge BACCOU

Merci pour cette question clé. Il est indispensable, devant un tel volume d'applications, de pouvoir effectuer un tri, notamment sur la base des impacts. Il faut absolument conduire l'« analyse d'impact » avec objectivité. Vous entendez parler régulièrement de *business impact analysis*, une expression dans laquelle le mot impact a son importance. Cet impact peut être financier ou non. Par exemple, pour une entreprise commerciale, la perte de millions d'euros est susceptible de mettre en péril la survie de l'entreprise.

S'agissant des impacts non financiers, il ne s'agit en aucune manière de mettre en danger la vie humaine, que ce soit celle des clients, celle des collaborateurs ou celle des usagers. D'autres enjeux ne sont pas spécifiquement financiers, tels que l'image.

L'objectivité est également de mise dans la classification des activités. Toutes les activités de vos organisations ne sont pas aussi importantes les unes que les autres. Il convient d'identifier les applications les plus critiques. Lorsque ces activités sont identifiées, vous pouvez en déduire les ressources nécessaires pour les poursuivre, quoi qu'il arrive. Il convient alors de s'intéresser aux applications, en lien avec ces activités.

Toutes les applications qui servent une activité ne sont pas critiques. La détermination des activités critiques réduit considérablement le nombre d'applications et de ressources informatiques critiques. La factualisation, avec des chiffres et une classification rigoureuse des activités et des applications, s'avère indispensable de ce point de vue.

Firouz MEGUEDAD

Merci. Je vous propose de passer à la séquence suivante afin d'aborder la question de l'audit du PCA.

Auditer son PCA

Julie-Anne PRUVOST
Chef de mission audit de performance, Safran

Véronique DEMACHY
Directrice associée, Mica

Julie-Anne PRUVOST

J'ai rejoint la Direction de l'Audit et du Contrôle Interne du Groupe Safran début 2010, après un parcours opérationnel de plus de 10 ans, dont une grande partie au sein du Groupe. J'ai exercé des responsabilités d'unité de recherche et de développement et des responsabilités de programmes aéronautiques à l'international.

Ma présentation a pour ambition de partager avec vous le retour d'expérience et les enseignements d'un audit PCA que nous venons de réaliser au sein du groupe Safran, et qui s'est terminé il y a quelques semaines.

I) Cadre et contexte du groupe Safran

Le groupe Safran est un groupe industriel avec trois branches d'activités :

- l'aérospatial,
- la défense,
- la sécurité.

Dans chaque branche d'activité, les contextes marchés, les demandes clients et les moyens industriels diffèrent. L'analyse d'impact stratégique doit donc nécessairement être adaptée à chaque secteur.

Le périmètre du groupe Safran est international : il regroupe près de 60 000 collaborateurs sur tous les continents, plus de 200 sites, dont 170 à vocation de production. Par sa nature et son implantation internationale, le groupe Safran présente une exposition naturelle à toutes les crises susceptibles de se produire autour du globe.

Vous avez évoqué Fukushima. Safran, comme d'autres groupes industriels, compte des collaborateurs et des activités au Japon. De même, s'agissant du « Printemps arabe », Safran possède des lignes de production en Afrique du Nord. Des événements moins médiatisés peuvent également impacter les opérations du Groupe : l'incendie d'une ligne de fabrication dans une usine, l'inondation d'un site industriel, etc.

II) Procédures de continuité d'activité au sein du groupe Safran

1) Premières mesures

Le Groupe n'a pas attendu l'accélération dramatique des crises de ces deux dernières années pour se poser la question de la continuité des activités. Pour un industriel, beaucoup de mesures de précaution peuvent être prises dès le démarrage d'un Programme, par « construction ». Ce sont souvent des mesures de bon sens. Pour un schéma industriel qui couvre plusieurs zones du globe et plusieurs sites de fabrication, nous nous posons la question de l'impact d'une crise majeure dans

une de ces zones ou de ces sites. Cela peut conduire à faire en sorte que deux lignes de production sur deux zones géographiques différentes soient capables des mêmes productions. De même, nous veillons à ne pas placer un moyen de production et un moyen de test au même endroit sur un site industriel, afin de disposer d'un moyen intact en cas de sinistre sur une partie du site, etc.

Cependant, malgré toutes les précautions de construction qui sont prises, il reste toujours un risque résiduel qui n'est pas couvert (catastrophes, etc.). Depuis 2009, la direction générale de Safran a donc décidé de lancer la démarche PCA.

2) Mise en place de la démarche PCA

La première procédure mise en place au sein du Groupe n'était pas nécessairement très opérationnelle, notamment parce qu'elle se basait sur une approche par processus. Elle avait toutefois le mérite d'exister. Le Groupe a procédé à un recensement, puis à un audit des PCA en 2011.

L'origine naturelle de la démarche PCA est le risk management. Il s'agit d'un moyen de traiter le risque d'indisponibilité partielle ou totale de l'environnement de travail habituel de l'entreprise. Il peut également exister d'autres *drivers*, qui incitent une société ou un groupe à s'interroger sur la continuité de ses activités :

- un évènement spécifique ;
- une demande du client : de plus en plus sensibilisés à la notion de continuité des activités, les grands clients peuvent demander à leurs fournisseurs de rang 1 de développer des solutions de continuité d'activité en cas de difficultés ;
- une prise de conscience et une demande de la direction générale.

Ce dernier point est le *driver* principal qui a conduit le déploiement et l'audit des PCA au sein du groupe Safran.

Avant de démarrer cet audit, nous avons ressenti le besoin très fort d'une étape « zéro », à savoir la formation de l'équipe d'auditeurs au PCA. Les deux auditeurs qui ont participé à ma mission ont suivi la formation, co-construite par l'IFACI et par la société Mica.

Nous avons également souhaité nous faire accompagner par un expert, afin de lancer la dynamique et de définir un vocabulaire approprié.

III) L'audit de la démarche PCA

1. Méthodologie d'audit employée

Nous avons retenu une approche pragmatique et concrète : qu'existe-t-il aujourd'hui au sein du groupe Safran en terme de gouvernance ? Les sociétés ont-elles décliné des procédures et écrit elles-mêmes des PCA ? Nous avons fait le tour des sociétés afin de récupérer les pratiques existantes.

Nous avons ainsi obtenu un panel de documents très divers, que cela soit en termes de contenu ou de maturité. Le vocabulaire était non homogène et parfois confus. Par exemple, un PCA nous renvoyait à un PCI, réduisant ainsi le PCA au volet informatique. Nous étions également renvoyés à des PSO (Plans de Soutien Opérateurs) qui recouvrent des demandes faites par le Gouvernement.

Véronique nous a aidés à établir un premier document de gouvernance, afin de poser les définitions, positionner les frontières entre les différentes activités et s'assurer que le socle méthodologique de notre audit était satisfaisant. Nous avons travaillé ensemble pour que les opérationnels du groupe puissent s'approprier le vocabulaire employé.

Le périmètre du groupe Safran est immense, alors qu'un PCA se développe pour un site ou pour une activité. Nous avons laissé pour l'instant le PCI de côté et avons décidé de ne pas traiter les plans de continuité d'activité les plus évidents (catastrophe naturelle, plans Grippe).

Une fois ce périmètre posé, nous avons établi un questionnaire pour procéder à un premier état des lieux. Ce questionnaire nous a permis de valider des points très importants : l'organisation, les rôles et les responsabilités. Un état des lieux du panorama des pratiques du groupe a ainsi été dressé, et des degrés de maturité divers au sein des différentes sociétés ont été déterminés.

A partir de ce panorama, nous nous sommes focalisés sur les sociétés que nous percevions comme les plus matures. Nous avons approfondi avec elles le détail des pratiques, la méthodologie et la réalité du PCA dans leur société.

L'apport de l'expert a été constant tout au long des étapes de l'audit : analyse de l'existant, établissement du premier document de gouvernance, élaboration du questionnaire, entretiens avec les opérationnels sur le terrain.

Véronique DEMACHY

Je m'attacherai pour ma part à commenter quelques points méthodologiques. A la lecture des documents du groupe Safran, très riches, il m'a d'abord semblé nécessaire de définir, par défaut, tout ce qui ne relevait pas du PCA. Nous avons reçu des PCI, des plans liés aux risques d'inondation, des dispositifs de gestion de crise qui ne relevaient pas du PCA, etc.

2. Définition des frontières de la démarche PCA

Le PCA n'est pas une cartographie des risques. Si je tiens à le préciser, c'est parce que nous avons reçu des documents traitant de scénarios, de risques fournisseurs, etc. Tous ces documents ne peuvent cependant être placés sous la bannière du PCA.

La définition du PCA que je vous présente aujourd'hui n'est pas universelle. De même, il n'existe pas de norme PCA en France. Nous nous basons sur les pratiques d'autres pays. Seul l'AFNOR cite le PCA en quelques lignes dans les normes 27 000, sans en définir les contours. Par ailleurs, la réglementation des banques nous a donné quelques définitions (Bâle 2 et Bâle 3), aux contours encore une fois indéfinis. J'utilise donc la définition qui a été reprise dans le guide de bonnes pratiques que nous avions édité avec l'AFNOR en 2008.

Il est logique de débuter la démarche par une cartographie des risques. Nous recensons les risques puis, face au risque d'indisponibilité partielle ou totale de l'environnement de travail, nous développons un PCA Le risque de continuité informatique et la communication de crise ne relèvent pas du PCA Ce schéma peut vous servir à définir des frontières de manière visuelle lorsque vous devrez exposer ces sujets à vos *risk managers* et à vos directions.

Avant de déterminer la démarche PCA, je me suis attachée à définir des bases, qui correspondent au développement du PCA Tout d'abord, il est important de déterminer un PCA pour chaque site qui héberge des activités critiques.

Certaines entreprises bâtissent des PCA par processus. Or, il est très difficile de le faire si le flux ou le processus se situe sur quatre ou cinq sites. Il est possible de reconstituer un PCA pour un processus, lorsque les PCA par sites ou par activités ont été réalisés. Malheureusement, la définition de Bâle 2 pour les établissements financiers recommande d'établir des PCA pour les processus critiques.

Je m'arrêterai sur la *business impact analysis*, que Serge a développée. On ne peut élaborer un PCA « en commandant » des listes d'applications critiques à son directeur informatique ou à son responsable PCA. Une analyse préalable des impacts des interruptions des activités est en effet nécessaire pour définir les activités critiques ainsi que leurs besoins de continuité humains et matériels.

La terminologie *business impact analysis*, très bien comprise en Angleterre ou aux Etats-Unis, a été parfois mal appréhendée par les entreprises françaises, ou raccourcie. Il me paraît donc important de parler d'« analyse d'impact des interruptions », des « activités » pour le PCA et des « systèmes d'information » pour le PCI.

Les opérationnels doivent définir les aspects critiques au sein de leur service. Dans une démarche d'entonnoir, seule l'essence vitale des activités est conservée. Pour mener une analyse d'impact des interruptions, il faut interroger et guider les métiers. Les experts PCA doivent prendre le temps de mener à bien une démarche face à face avec les opérationnels lors d'entretiens individuels. Le PCA est en effet construit à partir de la connaissance du cœur de l'activité détenue par vos opérationnels.

3. Les étapes de la démarche PCA

La démarche PCA que j'ai proposée au groupe Safran est en grande partie issue de la méthodologie que j'utilise depuis une quinzaine d'années pour bâtir des PCA dans tout type d'entreprise et dans tout pays.

Elle est fondée sur l'analyse et la cartographie des risques, pour être compris des *risk managers*. Par la suite, il convient de procéder à l'analyse des risques d'indisponibilité de l'environnement de travail.

Nous avons traduit l'analyse de l'impact des interruptions dans le jargon de Safran en analyse de l'impact *business* de ces risques, pour définir une stratégie de continuité d'activité. Ceci permet de définir le cœur des activités critiques et leur délai maximum d'interruption. Par la suite, il faut rechercher et chiffrer les solutions de continuité envisageables.

La démarche PCA est une démarche « à vie ». Si vous n'êtes pas à même de présenter des chiffrages, justifiés par des analyses d'impact, des interruptions à vos directions, les engagements ne seront pas clairs.

Puis viennent les phases d'implémentation et de formalisation. La formalisation de la procédure PCA intervient tardivement. Enfin, ont lieu les tests et la récurrence.

La direction doit s'impliquer dès le début du processus : elle doit se prononcer sur le périmètre des activités critiques et sur la stratégie de continuité (outils, personnes et matériel mobilisés), valider les budgets associés et définir chaque année les budgets associés aux tests de ces procédures.

Dans l'industrie et les services sont déterminés des plans de test sur trois ans et des budgets associés à des programmes de tests. Ces budgets sont votés, soit pour trois ans, soit chaque année en période budgétaire.

Lorsqu'une entreprise telle que Safran décide de tester la production d'une partie d'un moteur d'avion dans une autre usine, elle doit assumer des tests très onéreux. L'implication des directions est indispensable.

Au-delà de la définition, les auditeurs doivent sensibiliser les directions sur les arbitrages et les budgets à associer aux PCA. A l'heure actuelle, ces projets sont trop souvent traités avec des budgets officieux ou rattachés à l'informatique.

IV) Points clé du retour d'expérience de cette démarche PCA

Firouz MEGUEDAD

Julie, quels sont les points clés de votre expérience qu'il convient de retenir dans la démarche PCA ?

Julie-Anne PRUVOST

Je souhaite partager deux éléments avec vous :

- les apports de cet audit au sein du groupe Safran ;
- les suites à donner à cet audit au sein du Groupe.

1. Apports de l'audit

J'évoquerai d'abord la composante profondément didactique et pédagogique de l'audit, qui a repositionné les définitions, les frontières et la méthode. La procédure Groupe, créée en 2009, a posé la démarche et commencé à éveiller une prise de conscience plus aiguë au sein du Groupe. Elle se déclinait par processus et était donc, par nature, très lourde à mettre en œuvre, peu pragmatique et peu opérationnelle.

La démarche structurée et pratique par sites et par activités est plus susceptible d'être appropriée par un opérationnel de terrain. Elle est aussi beaucoup plus simple à mettre en œuvre.

Les présentations d'audit, à fort contenu pédagogique, ont rencontré beaucoup de succès au sein du Groupe. Elles sont déjà réutilisées de manière intensive, auprès de la direction des risques du Groupe et de la direction industrielle, pour former et sensibiliser à nouveau sur la problématique PCA et ses frontières avec les autres activités.

Nous prévoyons également de prendre contact avec notre université interne pour enrichir la formation des *risk managers*, voire créer un module PCA pour les managers opérationnels.

L'audit a également servi à casser certains préjugés sur le PCA, notamment la nécessité de gonfler artificiellement les stocks ou de doubler toutes les lignes de production. Implanter une démarche PCA n'est pas nécessairement coûteux pour toutes les activités. Les opérationnels doivent déterminer les éléments critiques, stratégiques, à couvrir au sein de leur société

La prise de conscience du temps et des moyens nécessaires pour déployer la démarche PCA a également représenté un apport important. Le *middle management* doit prendre en charge le PCA et non uniquement garantir ses performances quotidiennes. Si aucune ressource humaine ni aucun budget ne sont dédiés à la démarche, le déploiement devient difficile.

Par ailleurs, on ne saurait demander à un panel de directeurs industriels d'un groupe important de développer un PCA en deux mois.

A l'occasion de cet audit, est également apparue une prise de conscience du caractère transverse de cette activité. En particulier, les RH doivent être impliqués, car ils sont susceptibles de mettre en place des astreintes et d'envoyer des collaborateurs sur des sites de délestage. Doivent également être impliqués la direction des risques, la direction industrielle et la direction informatique, pour les données et les outils critiques.

Nous avons identifié quatre leviers majeurs au niveau du groupe Safran. Faute de temps, je n'évoquerai que les deux derniers : la sensibilisation et la formation, nécessaires pour bien implanter le vocabulaire et la démarche.

2. Suites à donner à l'audit au sein du groupe Safran

Si l'on considère les trois activités qui font l'objet de ce colloque :

- Dispositif de crise ;
- PCA ;
- PCI.

Des audits du dispositif de crise sont réalisés au sein du Groupe Safran depuis 2008, et nous venons de réaliser un premier audit des PCA. Au-delà d'un audit de suivi sur la problématique PCA

d’ici deux ans, on peut envisager d’adresser la maturité de la démarche PCI puis, la maturité étant atteinte sur ces trois activités, nous pourrons commencer à raisonner en transverse sur ces sujets.

Le plan de secours informatique

Mettre en œuvre un programme sur la continuité informatique

Fabrice CHATRON

Ancien chef de mission de l'I.G., Responsable continuité informatique, Groupe BNP Paribas

Firouz MEGUEDAD

Fabrice CHATRON interviendra sur la mise en œuvre d'un programme de continuité informatique. Serge BACCOU évoquera ensuite plus particulièrement l'audit du plan de continuité informatique.

Fabrice CHATRON

Je suis responsable du programme groupe sur la continuité informatique de BNP Paribas. J'ai construit ce programme, qui a été lancé en 2009, avec Serge BACCOU.

I) Raisons de la mise en place d'un programme sur la continuité informatique

L'informatique est un secteur incontournable pour l'activité bancaire. L'aspect continuité informatique était pris en compte dans l'ensemble des entités du groupe mais, en l'absence de référentiel commun, la cohérence d'ensemble n'était pas garantie.

Le programme vise à établir un set normatif pour cadrer la continuité informatique et traiter les problématiques de bout en bout. Par ailleurs, d'autres *drivers* existent, notamment les régulateurs, qui se montrent de plus en plus vigilants. Régulièrement, ils demandent des preuves de mise en place du dispositif de continuité informatique.

En outre, les clients deviennent de plus en plus exigeants. Cette caractéristique s'est renforcée depuis la catastrophe de Fukushima. Chacun a alors compris d'un coup qu'une région entière pouvait subitement rencontrer des problèmes. Il ne s'agit donc pas de conserver l'ensemble de ses actifs informatiques dans la même région. De plus en plus de clients demandent donc des *data centers* éloignés.

L'image doit par ailleurs être préservée. Les banques se montrent actuellement particulièrement attentives à ce sujet.

Enfin, nous nous sommes appuyés sur la communauté des auditeurs, qui donnent leur avis indépendants sur la question. Ils ont concouru à la création de ce programme, en montrant l'intérêt et le besoin de développer une approche relativement unifiée sur la continuité informatique.

II) Le positionnement de la continuité informatique par rapport à la continuité d'activité

La continuité informatique est englobée dans la continuité d'activité. L'activité relève des métiers, qui utilisent des *assets* informatiques. Les métiers ne voient que la partie immergée de l'iceberg : l'application utilisée quotidiennement. Toutefois, pour que cette application fonctionne, tout un écosystème (partie immergée) est nécessaire, qu'il n'est pas toujours aisé de distinguer.

La continuité informatique comporte une forte composante technologique. Les sachants sont essentiellement des informaticiens. En général, les décideurs proviennent également du domaine informatique. Or, il est très important de traiter ce sujet au plus près des décideurs.

C'est pour cela que nous avons mis en place des *information continuity officers*, au plus proche du DSI, qui assurent le lien avec la continuité d'activité. Ils identifient les *assets* critiques à observer ainsi que les ramifications informatiques pour les applications critiques.

III) La mise en œuvre du PCI

1. La classification des applications

Les deux niveaux qui nous intéressent en priorité sont les applications critiques et les applications importantes.

Nous avons déterminé un « thermomètre » commun à l'ensemble de l'Entreprise. Nous avons fixé des seuils d'impact financier et non financier, que nous remplissons avec les responsables d'activités concernés. Ainsi, nous obtenons une classification Groupe sur les applications, ce qui nous permet également de connaître les raisons pour lesquelles une application est critique.

L'enjeu principal de la continuité informatique renvoie à une question de moyens face aux besoins. Effectuer un travail préalable sur les impacts permet de calibrer la solution à mettre en œuvre.

2. Les RTO (Recovery Time Objectives) et les RPO (Recovery Point Objectives)

Le RTO représente le temps dont nous disposons pour mettre en place la solution de secours et revenir à une solution fonctionnelle.

Le RPO est connexe et concerne la donnée. Il s'agit du point temporel sur lequel nous sommes capables de revenir en matière de données. Les RPO traditionnels sont le RPO à un jour (retour sur les données telles qu'elles étaient sauvegardées la veille) et le RPO qui tend vers zéro (retour vers les données telles qu'elles prévalaient à l'instant de l'incident).

Nous avons ajouté la notion de besoin en sauvegarde restauration. Souvent, ce sujet est laissé aux productions informatiques, avec deux options :

- soit une sauvegarde totale ;
- soit la définition préalable des données nécessaires pour « repartir » d'un pont de vue informatique.

C'est cette deuxième option que nous avons choisie.

3. La continuité des données

Les données représentent l'actif le plus précieux de l'Entreprise. Lorsqu'une donnée client est perdue, par exemple à l'occasion de la perte d'un *data center*, elle ne peut être récupérée. Deux types de mécanismes pallient ce problème :

- la réplication synchrone ou asynchrone : elle consiste à dupliquer les données au fil de l'eau sur différents *data centers ;*
- la sauvegarde et la restauration.

4. Les data centers

En cas de perte d'un *data center*, deux approches sont développées :

- une approche application par application, qui détermine la marche à suivre pour chaque application ;
- une approche *data center* : elle indique la marche à suivre pour recréer la capacité de production informatique à un autre endroit dans des délais acceptables, en y associant les procédures appropriées.

Pour ne pas concentrer tous les risques sur un même *data center*, il convient de développer des stratégies sur deux *data centers*, voire plus.

La continuité informatique doit être assurée de bout en bout, en impliquant les métiers, les architectes, l'étude et la production informatique. Nous avons constaté que la continuité informatique était souvent adressée à la production. Cette façon de faire présente pourtant des limites. La production exploite ce qui lui est communiqué.

Ce programme s'est employé à rétablir les connexions aux différents niveaux afin que les différents acteurs se parlent et comprennent qu'ils font partie de la solution au problème. Ce sujet se traite en équipe de bout en bout.

5. Les anciennes applications

Le sujet des anciennes applications est souvent revenu. Pour reconstruire la connaissance de ces applications (parties immergée et émergée), il faut déterminer la manière dont elle s'intègre dans le système d'information.

Dans le programme, nous avons mis en place une méthodologie qui permet de revoir les applications et de poser le constat sur la continuité, ce constat étant présenté lors d'une *management review* avec le métier, l'IT métier et la production.

6. Le plan de secours informatique (PSI)

Le plan de secours informatique décrit les solutions à mettre en œuvre. Dans les descriptions des solutions de secours, nous avons déterminé deux niveaux :

- la description des solutions à notre disposition pour faire face aux incidents ;
- les procédures de production afférentes à ces solutions, qui donnent les instructions techniques détaillées.

7. Les ressources clé

Dans la continuité informatique, nous disposons de ressources clés. Reste à déterminer quelles personnes doivent être appelées et selon quel mécanisme. Les intervenants clés doivent être identifiés.

8. Les exercices

L'exercice est la seule preuve permettant de s'assurer que l'ensemble de la démarche a été effectué correctement. Sans exercice, il est possible de prévoir, voire de financer des solutions, mais sans savoir si celles-ci fonctionnent. L'exercice présente toutefois des risques ; il se décide souvent au plus haut niveau.

Nous avons introduit la notion d'exercice sur table : les procédures actuelles sont examinées avec les intervenants afin d'évaluer leur effectivité dans la réalité. En général, ces exercices s'avèrent assez révélateurs.

A un niveau intermédiaire, il est possible d'effectuer l'exercice complet ou des parties de l'exercice sur des environnements qui ne se trouvent pas en production. Enfin, au niveau le plus représentatif, l'exercice est réalisé en production.

9. Suivi du programme

En termes de suivi, nous prenons en compte :

- d'une part, l'aspect documentaire ;
- d'autre part, l'exercice (le résultat).

IV) Conclusion : les défis de la continuité informatique

La continuité informatique implique de relever plusieurs défis :

- traiter l'ensemble des problématiques organisationnelles, notamment en vérifiant l'effectivité des connexions à tous les niveaux ;
- outiller la démarche : nous avons mis en place une gestion électronique de documents qui permet de recenser l'ensemble des documents de continuité ;
- réduire le nombre d'applications critiques et justifier les raisons de l'aspect critique ou non ;
- trouver les bons interlocuteurs pour les systèmes d'infrastructures (métiers) ;
- clarifier les besoins et les impacts, pour fixer les budgets à mettre en place (ce point nécessite un fort soutien de la direction générale).

V) Questions

De la salle

J'ai été sensible à cet exposé, car je suis responsable du plan de continuité des activités à la Banque populaire.

Je souhaite revenir sur deux points.

Il est tout d'abord important d'identifier l'écosystème et le SI de manière précise, par une cartographie. Celle-ci est toutefois peu aisée à obtenir, en raison des interconnexions des systèmes informatiques. Ces interconnexions évoluant énormément dans le temps, je me demande si ce ne sont pas les exercices qui permettent la validation.

Par ailleurs, les solutions de secours informatique doivent être en adéquation avec l'expression des exigences métier. Or, des exigences peuvent être définies dans le cadre de contrats de service métiers. Au sein de BNP-Paribas, avez-vous engagé cette démarche ?

Fabrice CHATRON

Le premier sujet, qui concerne la cartographie complète avec les liens du système d'information, peut encore paraître utopique pour les informaticiens. Nous en avons connaissance, morceau par morceau. Toutefois, il reste assez délicat de le représenter par un référentiel commun ou sur papier. Nous effectuons donc des zooms sur des zones, en priorité celles qui sont les plus extrêmes pour nous. Sur ce sujet, nous montons progressivement en maturité.

S'agissant du deuxième sujet, les contrats de service, nous avons passé un long moment, au cours du programme, à interconnecter la communauté « continuité d'activité » et la communauté « continuité informatique ». Dans un premier temps, il est très important que ces acteurs prennent l'habitude de travailler ensemble. A l'origine, ces deux notions se touchaient sans être intégrées.

A l'heure actuelle, en termes de contrats, les maturités diffèrent selon les entités. Les entités qui étaient les plus matures sur ces sujets disposent déjà de contrats. Toutefois, le sujet doit encore progresser.

Pour ma part, je souhaite avant toute chose vérifier qu'une cohérence est assurée entre la partie continuité d'activité et la partie continuité informatique en termes d'expression des besoins.

De la salle

Au-delà de la coordination de l'activité informatique, lors de vos tests de bascule, intégrez-vous le personnel *business* opérationnel ?

Fabrice CHATRON

Tout à fait. Le personnel de la continuité d'activité doit être au courant de nos tests et de leurs résultats.

En termes de continuité informatique, différents niveaux de tests peuvent être déployés.

Le *business* intervient surtout sur les exercices en production. Des exercices de bascule plus ponctuels démontrent notre capacité de bascule. Nous faisons alors intervenir le métier. Tout ceci s'effectue en collaboration avec la continuité d'activité.

De la salle, France Télécom

Les tests sont-ils intégrés dans le PCI ou sont-ils définis par la suite ?

Fabrice CHATRON

Le PCI reprend les solutions. Face à lui, le plan d'exercice détermine les moments où les solutions ont été testées, leur résultat, etc.

De la salle

La mise en œuvre des exercices fait souvent l'objet de réticences. La continuité d'activité va de pair avec des catastrophes importantes.

Faites-vous des exercices qui portent sur une perte de l'ensemble du système informatique ou des exercices unitaires ?

Fabrice CHATRON

Nous pratiquons les deux types d'exercices. Je pense toutefois qu'il faut d'abord effectuer les exercices individuels avant de mener l'exercice global. Les entités les plus matures isolent un *data center* et vérifient que l'ensemble du système d'information fonctionne. Il reste assez difficile de viser l'exhaustivité.

Auditer son Plan de Secours Informatique et détecter ses vulnérabilités

Serge BACCOU
Directeur associé, Baccou Bonneville Consultants

Je commencerai cet exposé en évoquant une anecdote. Vous avez dû entendre parler hier de la panne de Free, qui a perturbé non seulement les utilisateurs mobiles de Free, mais aussi d'autres abonnés d'Orange. Cet évènement prouve que l'informatique est omniprésente.

Imaginez également qu'une banque ne soit plus capable de vous communiquer le montant de votre compte bancaire.

Au-delà de la plaisanterie, il existe de vrais risques systémiques. Certaines banques ont pris une part importante dans l'économie nationale et internationale. Elles sont considérées comme des acteurs systémiques : si elles venaient à rencontrer un problème informatique, elles pourraient engendrer des problèmes chez d'autres acteurs financiers. La crise serait alors équivalente à celle de Lehman Brothers, mais sous une déclinaison informatique.

Les actions des entreprises apparaissent nécessaires pour assurer la sécurité des personnes et des activités. Les actions menées au niveau de BNP Paribas dans ce sens ont demandé un investissement important. Plus de 1 000 personnes ont été formées à son programme de continuité informatique, dans le monde entier.

Le rôle de l'auditeur consiste à vérifier que les budgets et les efforts déployés sont en adéquation avec les enjeux.

I) Exemples qui ont servi à monter le programme de continuité informatique de BNP Paribas

La continuité informatique peut se baser sur des normes ou sur des bonnes pratiques internationales.

En particulier, la norme BS 25777 du *british standard* (organisme de normalisation au Royaume-Uni, équivalent de l'AFNOR en France) permet d'établir le cadre organisationnel d'un programme de continuité informatique.

Le *british standard* propose également un document de bonne pratique sur l'organisation des exercices, notamment sur des *data centers*.

La norme BS 25777 a inspiré l'ISO (organisme international de normalisation) pour créer une norme dans la lignée des 27 XXX (normes associées en général à la sécurité). En 2011, est sortie la norme 27 031 (norme sur la continuité informatique).

Par ailleurs, il existe de bonnes pratiques de production informatique : ITIL V3 consacre, dans son cahier *service delivery*, un chapitre sur la continuité informatique (IT *service continuity management*).

En tant qu'auditeurs, vous pouvez vous baser sur ces textes normatifs pour analyser la maturité de vos organisations. Dans le cadre de l'intervention que nous avons menée pour BNP Paribas, ces textes nous ont permis de gagner beaucoup de temps, car ils présentaient le menu des actions à réaliser.

II) Déroulement du PCI

La vérification de la présence des éléments organisationnels constitue le point de départ d'un audit.

1. *L'élaboration d'un document de politique de continuité*

La politique de continuité est un document visé en général par la direction générale, et approuvé par la direction informatique, qui explique les grandes lignes directrices de la continuité informatique.

Ce document a été réalisé pour BNP Paribas, en grande partie par Fabrice. L'informatique de BNP Paribas étant de nature fédérale, elle comprend de nombreux DSI (une vingtaine). Il a fallu convaincre ces derniers d'accepter cette politique de continuité. Elle les contraint à développer des solutions sur les actifs et les activités les plus critiques. L'absence de ce document fondateur prouve un niveau de maturité inférieur.

2. *L'attribution d'un budget*

Sans budget, il n'est pas possible de monter un projet de continuité informatique. Un budget de continuité informatique s'avère souvent conséquent.

Un auditeur doit s'intéresser au budget qui est consacré à la continuité informatique. Bien souvent, l'information est difficile à collecter.

3. *La nomination d'un responsable*

Dans notre cas, c'est Fabrice qui était responsable. En l'absence de responsable pour la continuité informatique, il existe une forte probabilité pour que le sujet ne soit pas traité correctement. Un patron de production informatique doit gérer une production au quotidien. Il ne peut s'occuper en même temps des cas de sinistres.

III) La détection des vulnérabilités

1. *La Business Impact Analysis (BIA)*

Il convient d'analyser tout d'abord les activités critiques, les lieux de production, les ressources humaines et les ressources informatiques. Un lien doit être établi entre les activités critiques et les ressources informatiques.

Lors du démarrage d'un audit sur la continuité informatique, il convient ensuite de vérifier les points suivants :

- l'existence de la BIA ;
- la criticité des activités ;
- le listage des ressources informatiques nécessaires aux activités critiques ;
- le cas échéant, la précision et l'exhaustivité de cette liste ;
- la définition correcte et réaliste des besoins en continuité (RTO et RPO).

2. *Le Single Point Of Failure (SPOF)*

Pour les systèmes les plus critiques, il faut doubler au maximum les équipements (serveurs, matériels réseau). Si le matériel réseau non redondé tombe en panne, il est considéré comme un *SPOF* : le maillon faible de la chaîne informatique. La « chasse aux *SPOF* » prend un certain temps et impose la cartographie de l'ensemble des équipements. Elle vise à identifier l'élément manquant.

Un auditeur peut également procéder à des vérifications très simples en bâtissant un tableau à deux entrées :

- une entrée « équipements nominaux » ;
- une entrée « équipements de secours ».

S'il manque un élément dans la colonne « secours », c'est le signe que l'on est en présence d'un *SPOF*. Avec des moyens simples, il est donc possible de vérifier si un plan de secours informatique est de bonne qualité.

Un plan de secours informatique n'évite pas nécessairement les *SPOF* : certains maillons faibles peuvent ne pas avoir été identifiés.

3. Les systèmes virtualisés

Les systèmes virtualisés, représentés sous la forme de petits serveurs, prêtent à confusion dans l'analyse de la continuité informatique. Il faut ici s'attacher au niveau physique et non logique. En effet, si le serveur nominal et le serveur de secours sont hébergés sur le même serveur physique, une panne de ce serveur entraîne une panne de l'ensemble des deux.

4. La récupération des données

L'audit des données est fréquemment oublié dans un plan de secours informatique. Les mécanismes de réplication et les mécanismes de sauvegarde font également souvent l'objet d'un amalgame.

Le mécanisme de réplication traite de nombreuses problématiques, notamment la panne d'un disque ou d'une baie de stockage. Avec un mécanisme de réplication synchrone, les données se retrouvent sur une autre baie de stockage, et si possible sur un autre *data center*.

Pour traiter les problématiques de corruption de données, la réplication n'est toutefois d'aucune utilité. La corruption de données est elle aussi répliquée sur la baie de secours en l'espace de quelques millisecondes. Elle se traite donc avec un mécanisme de sauvegarde et de restauration.

5. L'obsolescence matérielle et logicielle

La probabilité pour qu'un matériel ancien tombe en panne est beaucoup plus forte que pour un matériel récent. L'obsolescence matérielle doit de ce fait être régulièrement contrôlée.

Il en va de même pour l'obsolescence logicielle. En cas de problème, un logiciel qui n'est plus supporté par un éditeur bloque toute possibilité de support.

6. La performance

Des saturations de serveurs peuvent survenir.

J'ai piloté une crise pour Danone dans les pays émergents : dans ce cas, le problème de continuité informatique concernait la performance et la saturation. Les pays émergents n'avaient pas suffisamment prévu la croissance des volumes. Les systèmes sont donc arrivés à saturation et sont tombés en panne.

7. Les failles de sécurité

Les failles de sécurité peuvent entraîner des dénis de service, et donc un problème de continuité informatique, susceptible d'impacter la continuité de service pour l'entreprise.

8. Confusion des termes

La filière SSI (sécurité des systèmes d'information) utilise l'acronyme DICT (Disponibilité, Intégrité, Confidentialité, Traçabilité). La « disponibilité » est le sujet de la continuité informatique. Certains parlent de la « disponibilité », alors que d'autres évoquent la « continuité ». On note cependant une grande confusion en la matière.

Je vous encourage à examiner d'éventuels liens avec la sécurité. Certains sujets, qui concernent la sécurité, ont des impacts sur la continuité informatique. Il faut qu'ils soient traités en commun.

IV) Recommandations

L'auditeur doit déterminer si les audits sont représentatifs.

L'exercice doit être pratiqué de manière régulière. La recommandation est fixée à au moins une fois par an pour les systèmes les plus critiques.

Il est également recommandé de dresser un procès-verbal de l'exercice signé par les différents acteurs.

Certaines entreprises subissent des pannes informatiques alors même qu'elles avaient réalisé des exercices. Ceci prouve que l'exercice ne constitue qu'une première étape. La gestion de crise implique de s'adapter à des circonstances qui n'avaient pas été imaginées.

V) Maintien en conditions opérationnelles du plan de secours informatique

Le maintien des documents et des cartographies constitue un véritable défi. Nous allons certainement progresser sur ce sujet. A l'avenir, vous entendrez de plus en plus parler de cartographie ou de CMDB : des outils dont les productions informatiques se dotent progressivement en vue d'une gestion plus automatisée.

Il est possible d'automatiser la collecte de ces changements et de construire les cartographies de manière plus automatisée. Pour autant, un plan obsolète n'est d'aucune utilité lors d'une crise et est même susceptible d'entraîner d'autres dommages, notamment en cas de bascule d'un mauvais serveur.

VI) Lien entre la gestion des incidents et la gestion de crise

En tant qu'auditeur, vous devez vérifier si le lien entre la gestion des incidents et la gestion des crises est en place. La gestion des incidents est traitée au quotidien par les informaticiens.

Heureusement, tous les incidents informatiques ne se transforment pas en crises. Lorsque tel est le cas, il s'agit de bien identifier lesquels sont susceptibles de se transformer en crises, et de déclencher au bon moment les bonnes escalades.

Le temps est un élément important dans la résolution d'une crise, en particulier dans l'hypothèse d'une crise informatique. Très souvent, les informaticiens ont le réflexe de vouloir trouver une solution au problème initial, au lieu de basculer sur un système de secours.

Le niveau de service toléré a également son importance : en deçà d'un certain niveau de service, il faut déclencher le plan de secours.

VII) Conclusion : le rôle de l'auditeur

L'auditeur doit sensibiliser la direction générale, qui n'a parfois pas conscience de l'importance prise par l'informatique dans les entreprises.

L'auditeur doit également « sortir du *corner* » la direction informatique, pour reprendre une image de boxe. Les directions informatiques sont souvent victimes de restrictions ou de contraintes budgétaires qui ne leur permettent pas d'assurer la continuité informatique ou de lutter contre l'obsolescence matérielle ou logicielle. Des rattrapages s'avèrent alors nécessaires.

La direction informatique ne doit pas s'en sentir responsable : elle ne pourra pas nécessairement réaliser l'ensemble de ces rattrapages sur son budget propre. Une réallocation de budgets pourra être utile pour moderniser certains systèmes et les aligner sur les besoins de continuité.

L'auditeur doit par ailleurs renforcer les liens entre PCI et gestion de crise.

Enfin, un audit, bien souvent, permet de lancer ou de relancer un projet sur la continuité informatique et de mieux le structurer. C'est fréquemment par un audit que la direction générale prend conscience de ce sujet et alloue des moyens pour résoudre le problème de la continuité informatique.

VIII) Questions

De la salle

Pouvez-vous nous donner une idée du budget moyen nécessaire pour assurer la continuité informatique, notamment en proportion des coûts d'exploitation habituels ou des investissements récurrents ?

Serge BACCOU

Cette problématique varie d'une entreprise à l'autre. Le niveau d'interpénétration entre l'informatique et l'activité peut être plus ou moins fort. Dans le cas d'une banque, les budgets s'élèvent à des dizaines de millions d'euros.

Par ailleurs, les grosses masses budgétaires sont en général dédiées aux investissements informatiques, indépendamment du programme de continuité informatique.

Pour répondre plus précisément, le programme sur la continuité informatique de BNP Paribas inclut une centaine de personnes à l'échelle mondiale ; 1 000 personnes ont été formées à la continuité informatique.

Ces moyens doivent être adaptés à la taille de vos organisations et aux enjeux informatiques.

De la salle

Je souhaite revenir sur les trois points sur lesquels porte le travail de l'auditeur : la politique, le budget et le responsable. J'ai découvert qu'il existait des responsables de PCA dans certaines entreprises, ce qui n'est pas le cas dans la mienne.

Où se situe ce responsable dans l'organisation de l'entreprise, lorsqu'il existe ? Quels sont ses moyens réels ? Dispose-t-il d'un budget ?

Serge BACCOU

Une organisation idéale comprend à la fois un responsable PCA et un responsable de la continuité informatique.

La personne en charge du PCA s'occupe du secours au niveau des bâtiments. Quant à la personne en charge de la continuité informatique, elle est souvent logée au niveau de la direction informatique, car les enjeux, les considérations techniques et les budgets y sont souvent localisés.

D'autres types d'organisation se font jour. Parfois, la continuité informatique est logée au niveau de la sécurité, en particulier celle des systèmes d'information. J'y vois un risque : les personnes de la sécurité risquent de négliger le dossier de la continuité informatique et les cas de sinistres, désastres, etc.

L'exemple de BNP Paribas n'est pas isolé. Le rôle de responsable de continuité informatique est très développé. Il faut toutefois y consacrer un budget.

De la salle

Je souhaite revenir à votre entrée en matière sur Free. Ces derniers temps, nous entendons beaucoup parler des problèmes subis par cette entreprise. Il y a quelques années, un autre opérateur a connu une panne importante. Un troisième opérateur subit lui aussi des pannes occasionnellement : toutefois, étant donné qu'il maîtrise parfaitement sa communication, nous n'en entendons jamais parler.

Je pense que la maîtrise de la communication et le regard critique des auditeurs représentent des points essentiels de contrôle. En effet, par une bonne maîtrise de sa communication, il est possible d'éviter de monter des systèmes compliqués et coûteux.

Serge BACCOU

Vous avez totalement raison. La panne de Blackberry l'an dernier s'est avérée très néfaste pour RIM, la société qui le construit, en partie en raison d'une mauvaise communication. La société a, en effet, attendu trois jours avant d'expliquer la situation.

Aujourd'hui, RIM se trouve en grande difficulté. Il est question d'un éventuel rachat. Une panne peut donc entraîner la chute d'une entreprise.

Free nourrit de grandes ambitions dans le domaine du mobile. Si son image de marque est écornée par une piètre continuité de service, ses efforts commerciaux et marketing seront réduits à néant.

Si la communication a donc son importance, il convient également de savoir rétablir le service. J'ai remarqué que depuis quelques années, l'impatience des consommateurs est de plus en plus grande. Le *cloud computing* ne fonctionnera que si les gens ont confiance dans la résilience du nuage.

De la salle

Vous avez évoqué la réticence des services informatiques à basculer sur les PCA. Je conseille également à l'audit de s'intéresser à la partie « retour arrière » après une panne, qui est très délicate à mettre en œuvre.

Serge BACCOU

Vous avez raison. C'est important.

Firouz MEGUEDAD

Merci pour cet échange. Nous constatons que nous évoluons dans des secteurs économiques très sensibles. Il s'agit à la fois d'assurer la continuité du *business*, le service client et de préserver l'image de l'entreprise.

PCA et Gestion de Crise

Comment associer les deux démarches complémentaires : création d'un pôle PCA et Gestion de crise au sein d'Aéroports de Paris

Guillaume TIFFREAU

Coordinateur dispositif de crise et continuité d'activité Groupe, SMRR-pôle Défense, Crise et Protection, Aéroports de Paris

Bonjour. Je suis en charge, au sein d'Aéroports de Paris (ADP), à la direction sûreté et management des risques, de la coordination des dispositifs de crise et de la continuité d'activité au niveau groupe.

I) Présentation d'Aéroports de Paris

1) Activités traditionnellement connues

Aéroports de Paris est connue pour ses trois principaux aéroports : Roissy, Orly et le Bourget. Le Bourget est le premier aéroport européen d'aviation d'affaire. Il est non négligeable en termes de gestion de continuité d'activité. S'il est moins visible que les deux plates-formes principales, il développe pour autant un trafic très particulier : il gère principalement des vols de VIP ou de chefs d'Etat, ainsi que des rapatriements.

Les aéroports traditionnels, Roissy et Orly, constituent des lieux d'accueil par excellence. Nous avons battu notre record l'an dernier, avec 88 millions de passagers.

2) Autres activités

Nous développons également d'autres métiers, en lien direct avec le cœur de métier de gestionnaire de plates-formes aéroportuaires.

- **Les commerces et services**
  Nous développons des filiales de vente au sein des aéroports de prestations de *duty free*, des parkings, etc. Il s'agit de services que nous rendons aux clients *B to C*.
- **L'immobilier**
  Les terrains d'Aéroports de Paris constituent des réserves foncières importantes, sur lesquelles nous hébergeons des gares de fret et des bâtiments tertiaires.
- **Des activités connexes, exploitées à travers les filiales**
  Il s'agit d'activités en lien avec l'architecture et l'ingénierie (développement de constructions d'aéroports à l'international, etc.) ;

- **le management aéroportuaire**
  Nous développons des concessions d'aéroports à l'étranger, où nous intervenons pour leurs gestions et du conseil.
- **Les télécoms spécialisées.**
  Cette fonction était déjà intégrée à Aéroports de Paris avant la privatisation du secteur des télécoms. Nous avons développé nous-mêmes nos réseaux de télécom et de radiotéléphonie sur les aéroports. Cette prestation est vendue sur les plateformes parisiennes et s'exporte à l'étranger.

Ce panorama vise à vous dresser l'ensemble des problématiques que nous pouvons rencontrer sur la gestion de crise et la continuité d'activité. Il existe des interdépendances très fortes, notamment avec la fonction télécom : c'est notre filiale qui est notre prestataire de services, mais aussi prestataire d'autres intervenants majeurs des plateformes, tels que les services de navigation aérienne.

Très récemment, le Groupe Aéroports de Paris a également acquis 38 % de TAV, groupe de gestion aéroportuaire Turque qui gère notamment l'aéroport d'Istanbul. De ce fait, Aéroports de Paris acquiert une dimension internationale encore plus forte, qui engendrera probablement un redimensionnement de la gestion de crise et de l'audit.

II) Organisation d'Aéroports de Paris sur la gestion de crise et la continuité d'activité

Aéroports de Paris, entreprise publique jusqu'en 2005, et société anonyme depuis, a connu une période charnière en 2003 : la « crise de la neige ». Celle-ci a donné lieu à une véritable « révolution » interne. Les équipes ont beaucoup œuvré pour la continuité du service aérien, mais cela n'a pas été perçu comme tel par l'opinion publique.

Cet évènement a donné lieu à la mise en place d'un responsable de crise interne, chargé de mettre en place un dispositif global sur l'ensemble des métiers (exploitation, techniques, interfaces, etc.).

Nous sommes partis d'une gestion opérationnelle du quotidien et des événements exceptionnels, pour nous orienter vers une déclinaison sur les risques opérationnels. En 2006, suite à la « crise des liquides » de Londres : Scotland Yard a demandé à l'autorité aéroportuaire de Londres d'interdire l'ensemble des bagages cabine pour déjouer un attentat terroriste.

Cet évènement a amené l'entreprise à s'interroger sur ses capacités à gérer une telle crise et à la résilience de ses installations. Les premières notions de PCA sont apparues à cette occasion.

En 2008, le département management des risques a été créé au sein de la direction de la sûreté. Après avoir lancé une méthodologie, une cartographie et un accompagnement des risques sur l'ensemble des entités (direction et filiale), nous nous sommes orientés vers une démarche de PCA structurée de manière globale.

En 2011 a été lancée une politique générale comprenant un référentiel commun de vocabulaire. Pour les directions opérationnelles, la continuité d'activité fait partie du quotidien. Elle consiste en un ajustement, en temps réel, des ressources aux pics de demandes et à la gestion d'événements particuliers (incident technique, bagage abandonnée, etc.). Il était donc nécessaire de bien définir ce que l'on met derrière le terme continuité d'activité.

A noter que la réflexion par site s'avère impossible. Nous ne pouvons privilégier un site par rapport à l'autre. Le trafic de Roissy représente deux fois celui d'Orly. Il est impossible d'imaginer une redondance de l'un par rapport à l'autre. Qui plus est, certains acteurs développent une activité dans nos infrastructures sans dépendre d'Aéroports de Paris directement. Ainsi, nous nous orientons vers une standardisation des procédures de nos activités en s'appuyant sur les systèmes de management intégré existants.

Comment associer les processus lors d'une simulation de crise ?

Catherine PIEDNOEL
Directrice associée, Arjuna

A la différence d'un PCI ou d'un PCA, la gestion de crise ne peut être simulée en réel. Certains s'y sont pourtant essayés provoquant des dérapages médiatiques lorsque l'exercice a été durant quelques instants pris pour une crise réelle.

Ces exercices nécessitent donc un cadrage précis en amont, car les risques de dérapage sont importants.

I) Définition d'un dispositif de crise

Un dispositif de crise comprend quatre piliers :

- le cadrage stratégique : il fixe les volontés des décideurs et des dirigeants en termes de remontée d'informations et évalue le niveau de crise ;
- l'organisation, les procédures d'alerte, les procédures de gestion de crise, les procédures et outils de communication, etc. ;
- l'entraînement ;
- la dynamique : il s'agit de la mise à jour et du maintien du processus.

II) La détection des signes avant-coureurs et l'organisation de la veille

Il existe plusieurs types de veille : réglementaire, technique, concurrentielle, médiatique, réseaux sociaux, etc.

Chaque entreprise doit développer des indicateurs qui lui permettent de repérer des dysfonctionnements. Dans l'agroalimentaire, par exemple, il peut s'agir de l'augmentation des plaintes des clients pour des problèmes de qualité.

L'interconnexion entre les sites, les BU, les filiales et le siège est un phénomène à prendre en compte pour que l'alerte et la mobilisation soient les plus rapides possibles.

En externe, les activités liées avec les autorités (portuaire, nucléaire, etc.) doivent envisager leur fonctionnement avec les autorités (obligations d'alerte, etc.).

III) Les procédures de crise

Je ne reviendrai pas sur la procédure d'alerte, qui paraît désormais claire, même si elle est souvent difficile à mettre en place (cadrage avec les opérationnels et la direction générale, fixation du moment à partir duquel commence la gestion de crise, mise en place des équipes chargées de trier les événements indésirables et les alertes, etc.).

Dans vos organisations, peut-être avez-vous vu arriver des tableaux « occurrences gravité, probabilité » ? Nous sommes sortis de la logique des tableaux et de l'évaluation de la gravité pour nous orienter vers une petite équipe d'évaluateurs.

Des experts de la qualité et des équipes de gestion de crise sont mobilisés. Certains sont chargés de recueillir au quotidien l'ensemble des alertes et de faire correspondre à chaque alerte l'organisation adéquate.

Nous travaillons sur les procédures de crise à chaque niveau. Le modèle de la cellule de crise tend à disparaître, au profit d'équipes de crise, qui travaillent à différents niveaux : sur le terrain, dans une BU, à l'étranger, etc. Il faut anticiper cette organisation en fonction des risques. La nomination de la personne chargée de piloter la cellule de crise est très importante.

Il existe encore des procédures de crise écrites, où le pilote de la cellule de crise est le PDG tandis que la cellule elle-même est constituée par le comité de direction. Dans des moyennes ou des grandes PME, ces dispositifs continuent d'exister, même s'ils sont inopérants.

Il faut réfléchir en amont à la différence entre le PDG, qui prendra la décision ultime, le pilote de la cellule de crise, qui coordonnera les opérations le moment venu, et les missions, qui émergeront en cas de crise ; par exemple, celle de coordinateur de la cellule de crise, garant du bon fonctionnement de l'équipe, ou le livre de bord. Le nombre d'informations échangées à un instant T lors d'une crise étant énorme, un livre de bord paraît en effet nécessaire pour suivre les opérations.

Les procédures médias et gestion des réseaux sociaux nécessitent également des procédures, afin d'être activables à tout moment.

IV) Les différents types d'exercices de crise

Il existe de nombreux types d'exercices de crise, selon la maturité de l'entreprise et les objectifs, des exercices sur table jusqu'aux exercices en vraie grandeur, sur plusieurs jours. Plusieurs écoles se distinguent dans ce domaine, notamment celles qui pratiquent l'exercice « électrochoc » (ceci fonctionne en l'absence de prise de conscience de la part de la direction générale).

Les exercices de crise impliquent de simuler les parties prenantes externes. En effet, la gestion de crise devient difficile dès lors que le monde extérieur en est informé. Les appels de clients, de médias et de l'interne sont donc simulés. L'équipe dirigeante est alors mise sous pression : en plus de gérer les aspects techniques de l'événement, elle doit également gérer les parties prenantes.

Différents types d'exercices peuvent être menés :

- exercice centré sur l'équipe dirigeante ;
- exercice qui teste tout ou partie des plans de secours : pour une des régions de la BPCE, l'exercice de crise a impliqué l'évacuation d'une partie des équipes qui ont activé le plan de secours ;
- exercice qui implique à la fois les équipes dirigeantes, des plans de secours opérationnels et les autorités.

V) Le cas d'ADP

Guillaume TIFFREAU

Au niveau d'ADP, la continuité d'activité n'était pas perçue comme étant prioritaire ou comme nécessitant un déploiement instauré par une direction fonctionnelle.

Nous avons utilisé les exercices de crise, qui incluent la direction générale et les BU. Nous en menons un par an, ce qui entraîne plusieurs mois de travail. Parallèlement, nous effectuons des tests : déploiement de basculement d'un centre informatique à un autre, mise en place de moyens de secours, etc.

Connecter le niveau de la direction générale, la direction de l'aéroport de Roissy et les niveaux opérationnels des différentes directions est assez exceptionnel.

Parmi les objectifs poursuivis, la continuité d'activité n'était pas présente. Nous suivions des schémas classiques : activer les deux cellules de crise, les relations inter-entités et tester la communication de crise.

1. Exemple de l'épisode neigeux

Lors de faits passés, ADP a été quelque peu maltraité médiatiquement. Tant de personnes s'expriment à notre place que nous ne nous faisons pas entendre de manière très positive. Par exemple, lors de l'épisode de neige de 2010, il a beaucoup été question des 2 000 ou 3 000 personnes qui ont dormi dans nos aéroports. En revanche, nous n'avons pas du tout entendu parler des 180 000 qui avaient réussi à partir ou à rejoindre leur destination. Globalement, nous avons pourtant assuré 80 % de notre trafic.

Pendant les trois semaines de l'épisode neigeux, la cellule de crise est restée ouverte en continu. 12 personnes travaillaient 12 heures d'affilée, puis se reposaient 12 heures. Nous sommes cependant parvenus au bout du système. Par chance, aucun accident n'est survenu. Les stocks étaient pourtant arrivés à leurs limites.

Notre plan de service hivernal est un plan de continuité d'activité. Nous sommes dimensionnés face à un niveau de risques. Nous sommes passés de quatre à cinq jours de neige intense à la possibilité de parer à sept jours de neige intense, soit un scénario qui a été pratiquement doublé.

Le niveau de glycol (produit qui nous aurait fait défaillance) ayant considérablement baissé, nous avons dû en faire acheminer le 24 décembre depuis Amman et les Etats-Unis.

Au premier COMEX de début janvier, l'entreprise s'était mise en ordre de marche pour qu'à l'hiver 2011-2012, elle puisse faire face à sept jours de neige intense. Actuellement, 3 millions de litres de glycol sont utilisés, soit 60 % de la production annuelle européenne.

Notre couverture de risques est totalement discutable. Notre directeur financier a émis des avis à ce sujet. Le budget a suivi dans ce cas. Nous avons été éprouvés plusieurs fois par la neige. Les phénomènes météorologiques sont donc relativement pris en compte par l'entreprise.

Les crises techniques (systèmes d'informations ou ressources primaires) ont émergé beaucoup plus difficilement, pour deux raisons :

- Roissy se développant depuis le début des années 1970, un empilement de mesures (redondances électriques) a eu lieu ; d'où une connaissance parfois approximative de certains points de sorte que nous devons encore sécuriser certains éléments des couches techniques ;
- la climatisation représente un élément important pour nous, car elle refroidit des scènes informatiques majeures sur nos sites (Nous nous sommes rendu compte qu'il s'agissait pour une fois d'un sujet sur lequel nous pouvions travailler tous ensemble, l'autre intérêt étant qu'aucun acteur public n'y était impliqué.).

Dès qu'un accident survient et qu'il cause des victimes, le préfet a autorité et devient directeur des opérations de secours. ADP se trouve alors dans une position totalement différente : l'appui aux opérations de secours.

Dans ce cas, nous étions totalement responsables. Il était donc beaucoup plus facile de « faire descendre » un flot médiatique, ainsi qu'un flot de clients, de prestataires et de tiers immobiliers.

Nous ne voulions pas tester notre résilience de la climatisation, car nous aurions rencontré un frein (réticences des techniciens, etc.).

Nous sommes donc allés rencontrer un agent technique, auquel nous avons demandé comment procéder pour couper la climatisation et avons tenté de déterminer quel serait le problème majeur susceptible de pénaliser nos installations. Le technicien, qui avait 30 ans d'ancienneté chez ADP, a pu répondre à toutes nos questions.

Une simple panne est constituée d'une rupture de vanne, qui fait tomber la pression du réseau de distribution. Automatiquement, les unités de production s'arrêtent. Toutefois, pour isoler la

vanne défectueuse, il faut trouver la fuite. Sur un réseau de 60 kilomètres, cela nécessite un peu d'organisation.

Nous n'avons pas testé l'ensemble des aspects techniques de la continuité d'activité, mais seulement examiné la recherche de fuites. Lorsque l'indicateur de chute de pression tombe, il faut appeler les agents pour qu'ils se rendent à des points stratégiques du réseau et qu'ils convergent.

En revanche, nous n'avons pas du tout joué le déploiement des moyens de secours. Dès lors que les groupes autonomes de climatisation parvenaient à se rendre dans la pièce appropriée avec la bonne clé, nous n'avons pas mis en marche les moyens de secours. Il s'agissait en effet simplement d'un premier exercice.

Le directeur général délégué participait réellement à la cellule de crise alors qu'en principe, ce n'est pas évident. Nous avons ainsi pu faire remonter de nombreuses problématiques.

2. Déroulement de la gestion de crise à ADP

Nous disposons d'une structure relativement classique. Une cellule de crise au siège d'ADP gère la stratégie de crise et l'ensemble des enjeux dits « d'entreprise » : communication interne et externe, RH, directions support, qui apportent un soutien logistique ou humain et une expertise au niveau tactique. Le niveau tactique se situe au PC de crise à Charles-de-Gaulle qui présente la particularité d'être multi-acteurs. Dans cette cellule de crise, sont présents des membres de la police, de la gendarmerie et des services préfectoraux.

Nous ne pouvons donc pas du tout prendre certaines décisions d'entreprise à ce niveau, en raison de problématiques de continuité de trafic et de respect des obligations de sécurité et de sûreté. Nous avons donc dû scinder la cellule de crise en deux parties : l'une traite les enjeux propres à l'entreprise ADP tandis que l'autre prend en charge les enjeux aéroportuaires métiers. Le centre de commandement de la police de Roissy se trouve au même étage que notre PC de crise. Même si nous ne les appelons pas, ils viennent. Nous tentons de respecter chacun nos informations. ADP prévient la DGAC, qui prévient le Ministère des transports, qui prévient Matignon. De l'autre côté, la police prévient le préfet, qui prévient le Ministère de l'Intérieur, qui prévient Matignon.

Les trois principaux terminaux sont les suivants :

- CDG1 : complexe T1-T3 ;
- A : zone A-B-C-D ;
- E : Air France – Skyteam – EFG.

Nous sommes producteurs de notre électricité de secours. Nous fournissons un courant de qualité en provenance d'ERDF sur l'ensemble de la plateforme. Nos capacités de production s'élèvent à 40 Mégawatts. La réglementation aéronautique nous impose moins d'une seconde d'interruption sur le balisage (le balisage ne peut donc s'éteindre en moins d'une seconde). Ces capacités de production nous permettent de mettre en sécurité nos serveurs informatiques.

C'était la première fois que nous effectuions un exercice avec la Centrale Frigo Thermoélectrique (CFTE), intégrée avec des dimensions opérationnelles d'exploitation.

Nous avons joué sur deux tableaux :

- la résolution de la crise technique : détermination du temps de reprise, etc. ;
- le lien avec les opérationnels, qui développent des problématiques différentes.

Lorsque la centrale nous a indiqué que la climatisation repartait, elle voulait ainsi nous signifier que le réseau était sous pression et que l'installation était relancée. Lorsqu'un opérationnel indique que la climatisation repart, il attend du froid devant une grille. La continuité d'activité ne portait donc pas tant sur nos capacités techniques à faire face que sur la cohabitation de deux

mondes opposés. En crise, les focus s'avèrent totalement différents. Nous avons réussi à faire parler les différents interlocuteurs concernés de manière très concrète.

En partant d'un fait générateur, nous avons réussi à faire prendre conscience de la situation à des entités très opérationnelles. Nous avons volontairement mis en place trois opérationnels animateurs pour assurer l'animation « basse », car ils connaissent très bien le métier et la technicité. Sur le mode projet, 25 réunions de préparation se sont tenues, de mars à août 2010. Il a fallu rencontrer chacun. A cet égard, il n'existe que quatre grands centres, mais ils n'ont pas l'habitude de se parler.

Le temps de préparation a été pour nous, management des risques, une source d'informations impressionnantes. Ce prétexte nous a permis de travailler « en sous-marin » pour faire émerger la dimension technique, vitale pour l'entreprise.

Le principe de fonctionnement de l'exercice est le suivant : une cellule de stimulation principale, constituée de six animateurs (un animateur pour deux joueurs), envoie des *stimuli* (fausses dépêches AFP, faux mails, faux cabinets ministériels, etc.), avec la mention « exercice ». Nous plaçons cet exercice sous l'aspect ludique. Il est très important de faire passer le message en interne que nous ne sommes pas là pour évaluer les personnes individuellement sur leur capacité à prendre des décisions.

Il s'agit d'abord pour nous d'une formation par l'exemple. Une attachée de presse, qui revenait de six mois d'absence maladie, a fait son « baptême du feu » sur un exercice. Heureusement, car certaines des erreurs qu'elle a commises lors de cet exercice auraient été impardonnables en cas de crise réelle. Grâce à cette politique interne d'exercices, qui se présentent comme des entraînements appliqués, « la mayonnaise prend ». Nous recevons même des demandes de directeurs de crise, ce qui constitue le meilleur signe de reconnaissance.

Ces exercices demandent toutefois un travail important. C'est la raison pour laquelle les exercices majeurs, au cours desquels l'ensemble de la chaîne est testé, sont au nombre d'un par an seulement.

Il ne s'agit pas du seul exercice que nous menons. Cette année, la thématique sera SI. Si internet était coupé en France, comment fonctionnerions-nous ? Certaines personnes nous demandent en outre de réaliser des exercices sur des systèmes métier. Nous nous trouvons donc vraiment dans une bonne démarche d'évaluation.

Nos interlocuteurs ont compris qu'il valait mieux se confronter à des simulations de crise dans des modes cadrés, où ils ont droit à l'erreur, qu'à une situation réelle.

En 2011 a eu lieu le premier audit sur nos PCA : le rapport entre les PCA informatiques et les PCA métiers. Nous avons ainsi obtenu une comparaison objective. L'audit remonte au plus haut niveau de l'Entreprise et est suivi par le conseil d'audit rattaché au Conseil d'Administration. L'audit nous a permis de lancer l'année dernière la politique générale.

Catherine PIEDNOEL

Peut-être cet exposé vous éclaire-t-il sur les différents niveaux d'exercice : le test d'une application, celui d'une procédure de secours, d'une procédure de rappel et l'exercice de gestion de crise, qui combine les deux.

Guillaume vous a expliqué l'importance de la qualité du scénario technique. L'ensemble du processus de la chute de climatisation a été écrit, à la manière d'un script de film. Pour que les équipes entrent dans le jeu de l'exercice et que celui-ci soit le plus proche possible du réel, il faut que le scénario, en particulier en informatique, soit construit avec les opérationnels et les informaticiens : les opérationnels doivent pouvoir justifier d'un mauvais fonctionnement.

Les exercices présentent un intérêt en amont, lors de la construction du scénario. Par la suite, les exercices sont joués : des précautions doivent alors être prises pour qu'ils soient acceptés par les équipes. Ils doivent également être dosés. La cellule d'animation des exercices déroule un

scénario. Si elle constate que la cellule de crise est dépassée, elle ralentit le processus. Des observateurs peuvent décider d'arrêter un exercice pour préciser certains aspects, avant de le redémarrer. Un nom de code exercice est donné afin de ne pas confondre un exercice et la réalité. Ces exercices, s'ils sont insuffisamment cadrés, peuvent présenter des risques de dérapage.

La culture de crise implique également un débriefing, qui inclut un plan d'action et des recommandations comportementales :

- organiser l'équipe ;
- organiser et savoir conduire des points de situation, etc.

Il faut veiller à ce que les enseignements de l'exercice de l'année n soient intégrés lorsque les exercices de l'année N+1 sont préparés et partagés avec les « joueurs ». Dans le cas contraire, les défauts se répètent d'année en année, car les équipes se renouvellent et l'aspect comportemental n'a pas été transmis.

S'agissant des crises réelles, il convient d'intégrer la pratique de retour d'expérience, qui a rarement cours dans les entreprises en cas de vraie crise. Les vraies crises peuvent en effet présenter des scénarios traumatisants, sur lesquels les entreprises n'ont pas envie de revenir. Malgré tout, c'est ainsi que la culture de crise progresse.

De plus, il est important que le retour d'expérience ne se présente pas comme un règlement de comptes. Enfin, la formalisation de la méthode de retour d'expérience permet leur réussite.

Guillaume TIFFREAU

Notre politique en matière de retour d'expérience est très proche du référentiel audit. Nous développons deux vocabulaires distincts, car leur compréhension n'est pas la même par l'interne. Les retours d'expérience s'inscrivent dans une démarche continue ; ils sont anonymisés. Au contraire, l'audit est souvent vécu par beaucoup comme un contrôle de l'activité.

VI) Questions

De la salle

Vous avez souligné l'importance du livre de bord. Pourtant, votre présentation ne l'évoque pas. Or la capitalisation de l'information vécue en crise peut alimenter et aider la direction juridique à contrer d'éventuels contentieux susceptibles de survenir plusieurs années après la crise vécue.

Catherine PIEDNOEL

Le livre de bord devrait figurer dans le carré central, dans la « coordination ». Il fait partie de l'organisation de la gestion de crise. Différentes philosophies existent par rapport à ce livre :

- certaines entreprises refusent d'en tenir un, du fait des risques juridiques encourus ;
- d'autres prennent le parti de le conserver, car il permet de faire face à la masse d'informations issues des différentes entités de l'entreprise.

Il est souhaitable de former le personnel à la manière d'écrire un livre de bord. La direction juridique peut avoir à le relire. Tout dépend du type d'outil utilisé.

De la salle

Je ne doute pas qu'ADP développe une expertise en matière de sécurité et de continuité d'activité. Dans la gestion de crise, quelle est la part d'un cabinet externe dans la réalisation de l'exercice ?

Guillaume TIFFREAU

La première part est constituée par les moyens. Actuellement, nous sommes trois personnes à travailler à temps complet sur la gestion de crise. J'ai deux correspondants à Roissy et Orly. Un cabinet extérieur nous donne des conseils méthodologiques sur des exercices d'imageurs.

Par ailleurs, un intervenant extérieur peut se permettre de jouer le rôle d'un faux directeur de cabinet, en étant vindicatif à l'encontre d'un membre de la direction générale ou du COMEX, alors que très peu de personnes en interne peuvent le faire.

Le troisième intérêt réside dans le débriefing. Un discours tenu par un cabinet extérieur peut être perçu différemment.

Nous avons travaillé plusieurs fois avec Arjuna, ce qui nous a permis d'avoir une ouverture sur les pratiques des autres entreprises (Air France, SNCF, etc.)

Catherine PIEDNOEL

Nous voulions illustrer le retour d'expérience de la catastrophe du tunnel sous le Mont Blanc. Sous l'angle juridique, une des parties prenantes a été condamnée au motif qu'elle n'avait pas fait d'exercice.

Guillaume TIFFREAU

Notre juriste a mené une étude interne sur les attendus du jugement du tunnel du Mont Blanc. Le cadre rattaché au directeur de la sécurité a été disculpé, au motif que son devoir d'alerte avait été exercé, eu égard aux moyens dont il disposait. En revanche, son responsable a été poursuivi pour son manque de préparation et parce qu'il avait connaissance que des procédures étaient défaillantes ou non à jour, grâce à son subalterne et d'autres entités extérieures.

Nous réfléchissons beaucoup au devoir d'information que nous avons vis-à-vis de notre direction générale et des services d'Etat. La judiciarisation devient un enjeu très particulier dans le pilotage de crise.

Gestion de crise et continuité d'activité : retour d'expérience sur la stratégie développée face à une crise géopolitique de grande ampleur

Michel COUTY
COO fonctions de BNPP EGYPT lors des événements survenus en 2011, Groupe BNP Paribas

Je vais vous faire part de mon retour d'expérience. En 2008, avec l'aide de Véronique, nous avons bâti un plan de secours. Les activités de *head office* de BNP Paribas représentent 750 personnes en Egypte, répartie sur deux principaux sites du Caire.

I) Retour d'expérience sur la gestion de crise de BNP Paribas lors des événements d'Egypte en 2011

La collaboration avec un consultant m'a conféré une crédibilité. La mise en place d'un plan de continuité d'activité nécessite de rencontrer les directeurs de départements. Les responsables d'exploitation (*back office* ou production) sont très sensibilisés à ces problématiques. Ils comprennent immédiatement les éventuelles conséquences d'une coupure de système. En revanche, il est plus difficile de convaincre le *middle management*. Or, le travail avec un consultant permet d'obtenir cette crédibilité.

Notre plan de continuité d'activité, dans le pire des scénarios, faisait en sorte que nous disposions d'au moins 75 positions. Nous avons trouvé un site de repli dans des quartiers sordides. Toutefois, il y a un an encore, Le Caire était l'une des villes les plus sûres au monde. Je n'avais donc pas prêté particulièrement attention à l'environnement autour de ce site.

1. Déroulement des événements

Les événements sont survenus très rapidement. Si certains avaient pu pressentir qu'une telle crise allait survenir, je n'avais pour ma part rien vu venir. Le mardi 25 janvier, journée de fête nationale, des manifestations étaient prévues, qui sont devenues très houleuses. La police a été très rapidement prise à partie. Le mercredi, des affrontements se sont produits, qui ont donné lieu aux premières victimes. Des véhicules ont été incendiés et des ministères attaqués (notamment le ministère de la communication et de l'information).

Le vendredi, jour de la prière, les manifestations ont commencé à se dérouler avec beaucoup de force. Avec la direction de la banque en Egypte et en France, j'ai alors pris la décision de lancer l'évacuation des expatriés et des personnes en mission sur place. Un malheur n'arrivant jamais seul, les autorités égyptiennes ont décidé de couper tous les accès internet et la communication mobile. Je n'avais pas prévu cette situation dans mon scénario. Il était impossible d'appeler les collègues et les personnes avec lesquelles il fallait prendre des décisions.

Le samedi 29, la situation s'est encore compliquée. Le centre commercial d'Arkadia, qui hébergeait nos activités de *back office*, a été pillé et incendié. Sur un effectif de 750 personnes, nous avons perdu 450 postes de façon irrémédiable.

Le dimanche, nous devions reprendre le travail. Par chance, la Banque centrale avait décidé de fermer les banques. Nous nous trouvions alors en plein marasme ; les chars étaient présents partout. Nous ne disposions d'aucune visibilité. Nous commencions à douter que la situation se redresse.

Le site de repli se situait juste en face d'un poste de police, qui jouxtait un centre télécom. Ce poste, comme l'ensemble des postes de police, a été incendié. Notre site de repli s'est donc retrouvé totalement inopérant. Quant à nos autres locaux, à deux pas de la place Tahrir, ils étaient devenus inaccessibles.

C'est alors qu'un couvre-feu a été instauré. Dans cette ville gigantesque, avec très peu de transports, nous ne pouvions convoquer les collaborateurs.

Très vite, les autorités ont décidé d'ouvrir les portes des prisons. Ce faisant, le gouvernement Moubarak cherchait à ce que la population demande la protection de sa police. En réalité, ce n'est pas ce qui s'est passé. Des bandits de grand chemin ont donc parcouru les rues et ont pu s'armer très facilement.

L'ensemble de nos collaborateurs, y compris les cadres dirigeants égyptiens, n'ont eu d'autre choix que de protéger leurs familles et leurs biens. Le management local ne pouvait consacrer son énergie et ses ressources à reconstruire les activités de la banque, car il passait ses nuits dehors. Des milices et des comités de quartier se sont créés pour que chacun puisse préserver sa famille, ses biens et son habitation.

2. *Mise en place et décisions de la cellule de crise*

Les collaborateurs égyptiens et le management local restaient donc chez eux. Nous nous sommes retrouvés à huit expatriés, puis à cinq, à l'hôtel Sémiramis près de la place Tahrir. C'est dans ces conditions que nous avons commencé à bâtir la cellule de crise.

La banque a été pillée et saccagée. J'ai trouvé une chaussure d'enfant dans le bureau du DRH, ce qui prouve que le pillage a été effectué en famille. Deux semaines après que les locaux ont brûlé, il régnait encore une odeur de cadavre épouvantable.

Nous nous sommes d'abord assuré que tous nos collaborateurs étaient sains et saufs. Une équipe de *call center* s'est cachée au moment où le centre commercial a été pillé, puis elle a réussi à s'échapper. Il n'a pas été aisé de réaliser un inventaire.

Les révolutions ne sont pas reconnues par les assurances. Par chance, la date officielle de la révolution en Egypte a été fixée après le 29 janvier. Dans ce domaine, il a fallu engager les démarches très rapidement. Pour pouvoir déposer un dossier auprès des assureurs, il est impératif d'enregistrer sa plainte auprès de la police. Or tous les bureaux de police avaient brûlé. Nous avons donc eu de grandes difficultés à trouver un commissariat de police dans lequel le préjudice subi par la banque pouvait être acté.

La communication interne et externe s'est avérée capitale, que ce soit vis-à-vis des collaborateurs ou de la direction générale. Des moyens importants doivent donc être alloués à cet effet. Sur les cinq personnes que nous étions, une passait son temps à communiquer avec la direction de Paris pour lui expliquer nos actions, la rassurer et demander son aide.

Un site extranet a été construit à cette occasion. La mise en place d'une communication protégée par mot de passe accessible librement depuis internet nous a été d'une grande aide.

Dans un contexte de ce type, sans visibilité, la première action consiste à maintenir le système à flot. En effet, si la banque avait commencé à couper les lignes de crédit accordées à d'autres banques de la place, elle aurait mis par terre l'ensemble du système bancaire.

Les activités suivantes nous ont paru prioritaires :

- garantir le paiement des salaires aux employés des entreprises clientes, en l'absence de cash ;
- alimenter les distributeurs en espèces ;
- donner la possibilité à la clientèle d'entreprise de déposer ses liquidités ;
- maintenir le *call center* ;
- développer une *task force* sur la problématique de recouvrement des prêts.

Il ne s'agit pas du tout de l'activité classique d'une banque. Nous imaginions que la situation économique allait se détériorer. Il nous fallait donc être parmi les premiers à mettre en place un dispositif fort pour obtenir le remboursement de nos prêts.

3. *Quelques images*

Des images des événements sont projetées.

Nous avions fait un trou dans le bureau du DRH pour évacuer ce qui pouvait l'être : des archives, une imprimante, etc.

Dans le parking de la villa de *Garden City*, nous avions enlevé toutes les voitures. Nous avons loué une des tentes qui sont utilisées lors des cérémonies de décès pour en faire notre salle d'archives.

Nous avons dressé d'énormes plans de travail, où les collaborateurs travaillaient les uns à côté des autres. A cet égard, il nous a fallu être très attentif au climat social. Les conditions de travail étaient en effet exécrables. Qui plus est, dans un environnement de révolution, tout est possible. La communication s'est avérée essentielle pour expliquer à nos collaborateurs qu'en réalité, tout n'était pas possible.

II) Principaux enseignements tirés de cette expérience

Dans une telle situation de crise, il m'apparaît essentiel de :

- photocopier tous les passeports et les visas des expatriés et des missionnaires ;
- disposer de cash en dollars ;
- avoir en sa possession un téléphone satellitaire ;
- réserver des billets d'avion *open* : Air France, partenaire de grande qualité, nous a expliqué comment mettre en place une *hotline* à ce sujet ;
- choisir des chambres d'hôtel proches de l'aéroport ;
- réunir les bonnes compétences (nous avons eu la chance d'être peu nombreux) ;
- adapter la liste des activités ;
- relocaliser le personnel ;
- partager les moyens : j'ai racheté 20 dollars des PC qui m'avaient été volés ;
- effectuer des tests régulièrement ;
- communiquer en permanence ;
- avoir toujours un plan de secours à disposition (plans A, B et C) ;

Depuis 2007, nous avions engagé la construction d'un nouveau siège au Caire. Or, il avait mis plus de temps que prévu à se construire. C'est aussi pour cela que nous nous sommes retrouvés dans une situation particulièrement difficile. Nous avons accéléré la livraison du bâtiment et commencé à déménager les premiers collaborateurs alors que nous étions encore en travaux. Nous avons ainsi pu maintenir le niveau de service auprès de notre clientèle.

Globalement, notre clientèle s'est montrée satisfaite des services que nous lui avons rendus dans ces temps difficiles. Nous travaillons aujourd'hui dans des conditions bien meilleures qu'avant la révolution.

III) Questions

Firouz MEGUEDAD

Dans la salle, avez-vous des questions sur ce retour d'expérience très animé et très vivant ?

Intervenant

Merci pour cet exposé très intéressant.

Je me demande si vous ne venez pas de nous faire la démonstration flagrante de l'inutilité de préparer un PCA, car vous avez su improviser sur le terrain. Je reconnais que ma remarque est quelque peu provocatrice.

Michel COUTY

Tout à fait. Si Véronique m'a convié aujourd'hui, c'est parce que nous avons été confrontés au *worst case scenario*. Nous avions quand même pu réfléchir sur ces problématiques avant la crise. Par réflexe, chacun avait rassemblé des numéros de téléphone et disposait d'un inventaire des responsabilités.

Vous avez raison. Néanmoins, je pense que l'on se sent moins démuni dès lors que l'on a acquis des réflexes au préalable.

Firouz MEGUEDAD

Pour poursuivre dans le sens de la réponse à la provocation, je dirais que ce n'est jamais ce qu'on prévoit qui se produit. En revanche, certaines actions doivent, quoi qu'il en soit, être menées de manière incontournable. Si elles ont été identifiées, planifiées et testées en amont, il ne reste à gérer que la particularité de l'événement.

Les forces de sécurité (police, gendarmerie, etc.) développent cette approche : plus la préparation est importante, plus le facteur humain peut être facilement géré.

Michel COUTY

J'ai oublié de préciser que certaines personnes ont contribué à sauver nos activités en Egypte, notamment le directeur de l'administration et le directeur de l'IT. Ces personnes se sont montrées admirables de courage. Elles ont notamment récupéré des serveurs qui nous ont permis de rebâtir notre *call center*.

Les exercices d'entraînement permettent d'identifier les personnes sur lesquelles il sera possible de s'appuyer en temps de crise. Dans ces périodes, les personnes exercent des métiers qui n'ont plus rien à voir avec leurs responsabilités d'origine.

Quels sont les risques majeurs à auditer en matière de PCA/PSI et Gestion de crise ?

Table ronde animée par François TABOUROT
Executive Vice-President, Mega International

Nathalie DROGUE
Responsable Audits Internes, Safran

Daniel NOUELLE
Responsable de l'Audit Informatique, Air France

David RIVIERE
Responsable de l'Audit des S.I., GDF Suez

Christophe SERRANO
Global Policies and Work Environment, Orange Business Services

François TABOUROT

Nous allons passer en revue l'ensemble du champ que couvre ce colloque. Les intervenants autour de moi vont répondre à des questions sur lesquelles nous avons travaillé ensemble, afin que vous ayez le point de vue de professionnels sur des problématiques simples et pragmatiques.

Madame la Présidente, en début de matinée, faisait état d'un constat partagé entre les professionnels : l'intensification de la fréquence et des conséquences des crises, dans le contexte de la mondialisation.

A Fukushima, on avait déjà remarqué des tsunamis d'une hauteur supérieure à celui qui est survenu l'an dernier. Leurs souvenirs étaient marqués par des pierres gravées sur des rochers de l'arrière-pays. Toutefois, lorsque le Japon a été inondé, il n'était pas le premier fournisseur mondial de l'ensemble des composants électroniques qui entrent dans la majorité de nos gadgets.

Je destine ma première question à Madame DROGUE : face à l'ampleur que prennent les conséquences des crises, quelle est la sensibilité des directions générales ? Quels sont les principes des dispositifs qui sont mis en œuvre dans vos organisations ?

Nathalie DROGUE

Je fais partie de Safran, groupe d'ingénieurs et d'industriels dans le domaine de l'activité aéronautique, défense et sécurité. Je suis responsable de l'audit interne, plutôt axé vers la performance et l'efficience des opérations, toutes activités confondues.

Tout a commencé en 2005, lorsque la direction générale a sollicité la direction risques management du groupe pour établir un référentiel de gestion d'alerte et de crise au sein du groupe.

La direction risques s'est appuyée sur son réseau de *risk managers* pour définir ce référentiel et le déployer dans l'ensemble des filiales du Groupe.

Avec Julie, nous travaillons sur plus de 200 entités, réparties sur une dizaine de filiales dites de « rang 1 ».

En 2008, la direction générale a sollicité l'audit interne, c'est-à-dire nous-mêmes, pour auditer ce dispositif, selon deux axes :

- analyser le référentiel ;
- donner l'assurance de l'implication des dirigeants dans ces dispositifs.

François TABOUROT

Monsieur RIVIERE, quelle est la sensibilité de la direction générale sur ces sujets et quels sont les grands principes du dispositif à GDF SUEZ ?

David RIVIERE

Je travaille à l'audit interne de GDF SUEZ, que j'ai rejoint en 2008 pour assurer la supervision des audits transverses Groupe sur les enjeux liés aux systèmes d'information et pour animer une filière d'expertise « Systèmes d'Information » au sein de l'audit interne. Auparavant, j'ai travaillé pendant 10 ans en cabinet (KPMG), où j'ai été amené à intervenir sur de nombreuses missions d'audit et de conseil sur des enjeux liés aux systèmes d'information, pour des clients qui relevaient essentiellement du secteur industriel.

La première crise que le groupe GDF SUEZ souhaite pouvoir maîtriser est l'accident industriel.

Le Groupe a redéfini son schéma de gouvernance sur la gestion de crise en mai 2010. Il a mis en place une structure de gouvernance qui permet d'assurer un pilotage continu, et non pas discret, des chantiers de mise en œuvre et de maintien des dispositifs de maîtrise des crises, à tous les niveaux de management du Groupe. Pour cela, il s'est appuyé sur deux fonctions centrales, qui possèdent des représentants à tous les niveaux de management du Groupe : centre, branches, BU et entités opérationnelles. Ces deux fonctions centrales sont la direction santé, sécurité et système de management d'une part, et la direction de la communication et de la communication financière d'autre part. Les missions de ces fonctions centrales consistent essentiellement à assurer la sensibilisation et la formation des entités opérationnelles, à organiser les tests, à développer et maintenir le référentiel Groupe de gestion de crise, et enfin à organiser la phase de capitalisation sur les retours d'expérience.

Dans ce contexte, l'audit interne intervient en complément et comme une troisième « ligne de défense ». Il se positionne de manière indépendante pour évaluer l'efficacité du dispositif de contrôle qui est porté par ces deux fonctions centrales. Il contribue également à l'enrichissement de leur référentiel, notamment en les sensibilisant à des scénarios de crise potentiels qui pourraient avoir été omis. Pour les scénarios de crise qui paraissent les plus sensibles, l'audit intervient pour corroborer les auto-évaluations qui ont été réalisées par les entités opérationnelles, en liaison avec ces deux fonctions centrales.

François TABOUROT

Monsieur NOUELLE, même question : quelle est la sensibilité de la direction générale et le dispositif en place à Air France ?

Daniel NOUELLE

Je suis responsable de l'audit informatique d'Air France.

Du fait de son activité, de son histoire et de l'étendue de son réseau, Air France a développé depuis longtemps une réflexion approfondie sur les crises.

La Direction générale est fortement sensibilisée à la continuité d'activité, aux crises et à leur gestion avec l'objectif d'assumer la responsabilité sociétale de l'entreprise, de préserver son image et d'assurer sa pérennité.

Le dispositif de gestion de crise peut répondre aux différentes situations envisageables. Chaque épisode est l'occasion d'évaluer l'existant et de rechercher toutes les améliorations possibles.

Actuellement le système de gestion de crise comprend :

- une procédure générale,
- un service de logistique de crise, responsable du développement des procédures, de la coordination avec les escales et les partenaires, du support de la cellule de crise, du programme des volontaires, etc.
- une cellule de crise activable très rapidement,
- un système informatisé de gestion de crise auquel sont reliées toutes les escales,
- un réseau d'expert de différents métiers dont le rôle est d'assister la cellule de crise dans l'évaluation de la situation, la recherche de solutions adéquates et la prise de décision,
- le support du Centre de Contrôle des opérations (en activité permanente 24/24),
- des dispositifs locaux dans chaque escale, rodés et activables immédiatement.

La politique de gestion de crise repose, entre autres choses, sur la recherche des meilleures pratiques et solutions avec des partenaires aériens, les autorités nationales et locales pour les escales et des grands groupes industriels ou de service. La logistique de crise donne toute son importance aux actions de formation des personnels impliqués (porte-parole, volontaires qui accompagnent les proches, experts métiers).

La continuité d'activité est organisée à la fois de façon centralisée (en particulier pour la coordination SI / métiers) et au niveau de chaque activité.

Les situations de crise, la continuité de service et les dispositifs de contrôle correspondants sont cités dans la cartographie des risques.

Nous avons réalisé des audits sur la gestion de crise (arrêt des vols en 2010 suite à l'éruption du volcan islandais) et sur la continuité d'activité. En particulier, nous avons travaillé sur les PSI.

François TABOUROT

Monsieur SERRANO, diriez-vous que la particularité du déploiement international d'Orange Business Services joue un rôle particulier, à la fois dans la sensibilité de la direction liée à l'activité et dans le dispositif mis en œuvre ?

Christophe SERRANO

Orange Business Services est un opérateur de télécommunications. C'est la branche de France Télécom Orange qui est dédiée au *B to B*. Nous avons pour clients les grandes entreprises de la planète. De ce fait, nous sommes extrêmement exposés à tous les risques, d'où qu'ils viennent.

En effet, nos équipements sont présents dans plus de 200 pays (tous les pays de l'ONU). Nous déployons des équipes dans 110 pays. Nos sites peuvent être très importants, tels que celui du Caire, qui comprend 1 400 collaborateurs. Nous développons donc une forte sensibilité aux risques de manière générale.

Par ailleurs, nous sommes l'opérateur de référence sur la partie France de France Télécom. Nous avons des obligations vis-à-vis de l'Etat, qui nous ont sensibilisés de tout temps aux risques et au PCA.

Même si nous développons cette sensibilité depuis toujours, une évolution assez récente nous a amenés à nous fédérer de manière plus homogène sur le problème des PCA : l'émergence des facteurs humains, la prise en compte des dangers massifs et des désastres physiques, naturels ou humains, dont l'un d'entre eux est l'émergence du H1N1.

Je vous rappelle que la grippe espagnole a tué plus de personnes en Europe et en Amérique que la guerre de 1914-1918. Nous ne pouvons donc totalement négliger ce type de risques. Nos équipes sont exposées dans le monde entier. Il ne faudrait pas qu'une partie importante de notre activité humaine se retrouve, du jour au lendemain, dans l'impossibilité de travailler. Cet aspect a donc été vraiment pris en compte.

Enfin, notre activité d'opérateur de réseau pur s'est développée sur les services, c'est-à-dire sur des hommes. Nous avons mis en place des centres dans le monde entier, avec des populations importantes. Nous avons, par exemple, développé quatre centres DMSC (support client) :

- un à Gurgaon, près de Delhi, de 1 000 personnes ;
- un au Caire, de 1 400 personnes ;
- un à Rio, de 800 personnes ;
- un à l'Ile Maurice, de 800 personnes.

Ces centres importants soutiennent chacun un gros quart de la population de nos clients dans le monde. Par conséquent, l'aspect humain a constitué un facteur déterminant. Nous sommes partis d'une prise en compte des risques techniques (coupures de câble, reroutage des données dans le monde entier). Aujourd'hui, avec l'émergence du facteur humain, nous nous orientons vers une approche plus fédérée : l'ensemble des risques sont analysés de manière cohérente et homogène. Cela nous conduit à mener une politique plus efficace dans ce domaine.

François TABOUROT

Nous avons entendu beaucoup d'histoires aujourd'hui, certaines aux conséquences dramatiques. Toutefois, nous avons du mal à croire qu'il serait aussi facile de mettre en place des dispositifs de crise ou des dispositifs qui assurent la continuité d'activité.

Dans la salle, nous nous sommes même interrogés sur l'intérêt d'organiser des dispositifs de recouvrement d'activités préparés et planifiés et sur la possibilité de laisser libre cours au talent humain au moment où les problèmes se posent.

Je vais à présent poser des questions, une nouvelle fois communes aux intervenants, relatives aux difficultés du dispositif qu'ils managent.

Les budgets alloués à ces dispositifs s'avèrent-ils suffisants ? Les personnes qui en sont responsables sont-elles suffisamment formées ? La direction générale, qui a été globalement présentée comme sensible à cette préoccupation, a-t-elle apporté son soutien ?

Nathalie DROGUE

J'identifie deux risques majeurs dans la mise en place de ces dispositifs :

- **Le manque de moyens, tant humains que financiers**
  Les notions de PCA ou de mise en place de dispositifs de gestion de crise renvoient à des actions de type préventif, pour couvrir un évènement dont l'occurrence est probablement très faible et l'impact très important. Un manager pourra vous dire que si aucune action préventive n'est menée, le coût d'un éventuel évènement sera exorbitant et que, dans le cas contraire, le coût sera immédiat. Toutefois, la probabilité d'occurrence d'un évènement ne doit pas intervenir dans la décision d'actions préventives.

  Cet investissement à long terme peut d'ailleurs être comparé à une forme d'assurance. Pour couvrir ce risque, il faut poser ce dispositif au niveau stratégique de l'entreprise, avec des points de validation à très haut niveau.

- **L'appropriation des méthodes**
  A Safran, la méthodologie et l'animation de la démarche sont pris en charge par la direction des risques groupe, associée à son réseau de *risk managers*. Les porteurs de rôles et les acteurs en cas d'événement sont les directions opérationnelles, qui s'avèrent beaucoup moins

disponibles. Elles devront pourtant assumer la responsabilité des événements en cas de crise. Pour couvrir ce risque, il faut insister sur l'aspect documentaire et sur les formations des dirigeants.

Daniel NOUELLE

Nous avons réalisé des audits sur les PSI qui ont été mis en place à Air France. J'identifie deux risques majeurs :

- **La compréhension de la nature d'un PSI**
  Un PSI ne garantit pas intégralement la disponibilité des systèmes d'information pour les métiers.

  Nous avons investi des moyens importants pour mettre en place des PSI. Pour les deux premiers sites de production en France, nous avons choisi une solution de haut niveau : en effet, les deux centres sont quasiment entièrement « clonés ». En principe, nous ne risquons donc pas de perdre des informations. Toutefois, si, par exemple, un bug intervient du fait de l'application d'un patch sur un système informatique, celui-ci s'arrête. Or, étant donné que toutes les données sont dupliquées sur le centre de secours, celui-ci est également affecté. Les centres de secours ne peuvent pas pallier les conséquences dues à l'évolution des systèmes (montée de version).

  Ainsi, le 29 juin dernier, nous avons vécu un arrêt système de près de huit heures qui a bloqué le départ d'une centaine de vols. A la suite de cet incident, qui a été expliqué, il a été décidé d'élaborer des PCA au niveau des métiers opérationnels majeurs qui sont complètement dépendants des systèmes d'information. Les métiers doivent définir un plan de continuité pour leurs activités critiques, pour les cas d'indisponibilité système.

  Nous sommes en train de développer des PCA dans les différents métiers qui n'en n'étaient pas encore suffisamment pourvus. Nous n'avons pas mis en place de coordinateur pour l'ensemble des PCA, mais nous en avons au moins un par métier. L'entreprise a consacré les moyens nécessaires à la mise en œuvre des PSI et des PCA. C'est au niveau du Directeur Général Délégué Opérations, qui chapeaute les métiers opérationnels, que sont suivis les différents PCA des métiers opérationnels. C'est également à son niveau qu'est prise en charge la procédure de gestion de crise que j'ai évoquée plus tôt.

- **le maintien en conditions opérationnelles**
  Il faut veiller à ce que les dispositifs de PSI et de PCA intègrent bien toutes les procédures pour le maintenir en conditions opérationnelles, faute de quoi l'investissement ne peut être rentabilisé.

François TABOUROT

Monsieur Serrano, quel jugement porteriez-vous sur les moyens qui sont alloués à la gestion de crise ou au PCA pour Orange Business Services, en particulier à l'occasion de la crise que vous avez partagée avec d'autres banquiers au Caire récemment ?

Christophe SERRANO

Au Caire, nous avons eu de la chance. Nous avons pu expérimenter notre mode de fonctionnement à cette occasion. Dans un réseau, il est assez facile de *back-uper* un site par un autre.

Les quatre centres de service clients que j'ai évoqués plus tôt couvrent chacun une zone géographique du monde : l'Asie, l'Europe, l'Afrique, l'Amérique, la France et l'Ouest de l'Europe. Lors de la crise du Caire, nous avons expérimenté le *back up* d'un site par un autre et le transfert de la charge, d'abord *a minima*. Le site du Caire a baissé sa productivité de 100 % à 20 % sur une dizaine de jours. Pendant 48 heures, le site a été complètement fermé : l'ensemble de l'activité a alors été basculé à Rio, à l'Ile Maurice et à Delhi.

Tout à l'heure, il était question de *war room* et de cellule de crise. A Orange Business Services, il est usuel d'organiser ce genre de dispositifs à distance, les parties prenantes étant situées à différents points de la planète. Une conférence téléphonique quotidienne de plusieurs heures nous a permis de nous organiser en temps réel pour basculer le *workload* d'un site sur un autre.

Globalement, le basculement de la charge de travail d'un site à l'autre s'est effectué à peu près correctement, même si de petits problèmes de langues se sont posés. Les clients se sont montrés satisfaits et conscients du travail accompli. Le PCA s'est avéré efficace à 98 %.

Nous avons toutefois atteint certaines limites. Ainsi, nous avons découvert qu'avec la bascule de la charge de travail, même en travaillant en mode dégradé, le transfert de charge sur les sites devenait très vite intolérable. A Delhi et à Rio commençaient à se poser des problèmes de capacité, de personnel et de présence. Un plan B s'avère donc de toute évidence nécessaire.

Par ailleurs, nous avions beaucoup compté sur le télétravail. Toutefois, l'ADSL et la téléphonie ont été fermés en Egypte.

Je retiens donc de cette expérience l'importance de bâtir un plan A, un plan B et un plan C, ainsi que l'importance du retour d'expérience. Nous avons su en tirer des leçons pour les crises ultérieures.

François TABOUROT

Je reviens à présent vers Monsieur RIVIERE pour aborder le cas particulier de son activité d'audit des PSI et des systèmes d'information. Suite à la présentation très nourrie de Monsieur BACCOU ce matin, j'en viens à penser que vous ne pouvez assurer cette mission qu'en connaissant bien l'architecture informatique et les architectures techniques.

Que pouvez-vous dire au sujet des compétences ?

David RIVIERE

Tout d'abord, j'ai trouvé la présentation de ce matin très complète de sorte que je crains de me livrer à des redites. Je vous propose donc de revenir sur les quatre points qui ont eu le plus d'écho par rapport à notre pratique de l'audit des PSI.

Ce matin, vous avez été plusieurs à insister sur l'importance des études d'impact. L'analyse de ce point est résolument inscrite dans notre approche d'audit car il nous semble que la meilleure façon de convaincre des directions d'agir dans le domaine des PSI est de se montrer très explicite quant aux conséquences métier d'une éventuelle indisponibilité du système d'information. Sur ce plan, nous travaillons à améliorer nos compétences.

Le deuxième point que j'ai relevé est le risque de déficit de couplage entre les PCA, les PSI et la gestion de crise. A l'audit interne, nous avons choisi d'apporter une attention toute particulière aux interfaces entre ces trois composantes, en sensibilisant nos collaborateurs à cet enjeu. Pourquoi travailler sur l'interface PSI-Gestion de crise par exemple ? Parce que nous avons observé que les engagements de RTO de nos PSI ne courent qu'à partir du moment où décision a été prise d'activer les PSI, et qu'il pourrait s'avérer plus long de prendre cette décision que de dérouler les opérations techniques de secours qui sont définies dans un PSI.

Le troisième point consiste à bien examiner la profondeur d'analyse des scénarios de panne ou de sinistre qui pourraient engendrer l'indisponibilité d'un système d'information et qui sont à la base des PSI. La revue de ce point nécessite une bonne capacité d'analyse des schémas d'architecture informatique. La profondeur d'analyse que nous demandons à nos collaborateurs réfère à trois aspects :

- **La prise en compte des infrastructures techniques sous-jacentes aux applications :** les branches qui s'appuient sur des centres de services partagés ont naturellement tendance à écarter le scénario d'une panne sur une infrastructure technique mutualisée, alors que ce scenario reste possible.
- **La prise en compte de l'intégralité de la chaîne applicative qui supporte un processus métier :** bien souvent, les études de scenario de panne / sinistre sont cloisonnées à une application particulière, sans tenir compte du risque de panne d'un système amont, qui aurait pourtant la même conséquence métier.
- **La prise en compte des limites des solutions de secours dites de « réplication » :** comme il a été indiqué ce matin, ce type de solution ne permet généralement pas de maîtriser une indisponibilité induite par une infection virale, et il nous semble approprié de le rappeler à nos interlocuteurs lorsque nécessaire.

Le quatrième point recouvre la réflexion préalable sur le séquencement du déclenchement des PSI applicatifs, dès lors qu'ils reposent sur une infrastructure mutualisée. En cas de panne d'une plateforme technique accueillant plusieurs BU, quelle BU faire redémarrer en 1er et sur quels critères objectifs ? Nous souhaitons nous assurer de la maîtrise de cette question dans notre approche d'audit.

François TABOUROT

Monsieur NOUELLE, je reviens vers vous sur la question des compétences spécifiques IT nécessaires à l'audit des PCI.

Daniel NOUELLE

Pour pouvoir travailler efficacement, il faut acquérir une pratique suffisante de l'audit des systèmes d'information. Il est préférable que l'équipe d'auditeurs comprenne au moins une personne spécialisée en informatique.

Nous avons réalisé deux audits de PSI, qui présentent trois axes majeurs :

- l'existence d'une stratégie décrite et validée au plus haut niveau pour mettre en place le PSI ;
- la solution mise en œuvre, de manière globale ;
- le maintien en conditions opérationnelles.

L'idéal est de développer des compétences informatiques suffisantes afin d'être à même de dialoguer efficacement avec le personnel des centres de production informatique.

Nous avons eu l'opportunité de pouvoir travailler à partir d'une liste des applications critiques qui existait déjà depuis 15 ans. A Air France, nous disposons d'environ 1 200 applications métier et d'une centaine d'applications techniques. Seules 5 % des applications métiers (une cinquantaine) apparaissent réellement critiques. Environ 70 à 80 applications sont sensibles.

Dans le cadre du PSI, nous souhaitions que la cinquantaine d'applications critiques redémarrent en moins d'une heure. Pour le millier restant, le délai de redémarrage est d'un mois au plus.

François TABOUROT

Vous êtes des professionnels de la communication : comment mettez-vous en œuvre cette capacité spécifique de votre métier, en particulier pour sensibiliser la direction générale à l'intérêt des PCA ?

Portez-vous les retours d'expériences ?

Nathalie DROGUE

Pour illustrer le rôle de l'audit interne, je m'appuierai sur la définition de l'audit interne telle qu'elle est défendue par l'IFACI : donner une assurance sur le degré de maîtrise des opérations au regard des risques évoqués.

Les animateurs des démarches sont-ils légitimes pour donner cette assurance au *top management* des sociétés et à la direction générale du groupe ? Je pense que non. En effet, on ne peut à la fois être juge et partie. C'est là que l'audit interne joue pleinement son rôle.

Pour apporter une sensibilisation importante auprès du management et des dirigeants, il convient d'auditer :

- **Le référentiel/ la documentation**
  La documentation doit être suffisante et suffisamment pertinente pour l'activité qu'elle doit couvrir. Si un évènement survenait au cœur des affaires des dirigeants, il faudrait leur rappeler les rôles et les responsabilités qu'ils doivent endosser.
- **Les plans de formation**
  Les dirigeants, peu disponibles, interviennent plutôt de façon ponctuelle dans la construction des PCA. Il est donc très important de mesurer le taux de couverture des dirigeants sur les plans de formation, en particulier sur la communication.
- **Les moyens matériels mis à disposition, à vérifier**
- **L'implication de la DRH (vérification des dispositifs d'astreinte et de la stratégie de continuité)**
- **La suppléance**
  Les suppléants doivent être formés au même niveau que les « titulaires ».

Il conviendra de s'assurer que les PCA ont bien été testés. S'agissant de la gestion de crise, l'auditeur ne s'interdira pas de réaliser une simulation de crise « surprise » pour tester les agissements de ses directeurs et managers.

François TABOUROT

Monsieur RIVIERE, quelle est la contribution de l'audit à la sensibilisation de la direction générale ?

D'autre part, l'audit interne participe-t-il aux tests des PSI ?

David RIVIERE

En termes de sensibilisation, je reviendrai à ce que je disais plus tôt au sujet de l'analyse des études d'impact, qui représente pour nous le point clé. Nous passons désormais 20 % du temps total de l'audit à l'analyse des études d'impact, et nous les challengeons. Pour ce faire, nous travaillons à faire intervenir des auditeurs qui connaissent bien le métier concerné : ce sont eux qui challengent les études d'impact ; la restitution en est rendue plus percutante.

Au-delà de la sensibilisation directe dans le cadre de missions d'audit spécifiques aux PSI, nous tentons de contribuer à la culture d'entreprise sur le sujet en intégrant un volet « prise en compte de la problématique PSI » dans tous nos audits de projets informatiques. Cette approche présente deux avantages :

- la récurrence du message ;
- la sensibilisation précoce des responsables de projet sur les coûts futurs qu'ils pourraient supporter s'ils ne prennent pas en compte la problématique du plan de continuité dès les phases amont du projet.

Vous avez par ailleurs demandé si l'audit interne participait aux tests : la réponse est non. Ce n'est pas l'option qui a été retenue par GDF SUEZ. Ce sont les deux fonctions centrales que j'ai mentionnées en introduction qui organisent les tests (sans être directement responsables de leurs résultats). Nous examinons alors deux points particuliers :

- les conditions de réalisation des tests, qui doivent être proches de la réalité ;
- une clarification sur les scénarios d'incidents qui ont été réellement testés et sur ceux qui ne l'ont pas été.

Daniel NOUELLE

S'agissant du test, l'audit n'y a pas participé. Nous avons simplement vérifié que les tests ont été effectués dans de bonnes conditions.

Il faut alerter la direction générale au travers des audits dans le cas où aucun plan de test n'a été prévu ou si le test n'est pas réalisé.

L'audit est chargé d'informer la Direction générale (comité exécutif) et le Comité d'audit sur la maîtrise des risques majeurs de l'entreprise. Notre plan d'audit est adossé à ces risques majeurs qui constituent près de 80 % des sujets de mission.

François TABOUROT

Monsieur SERRANO, pensez-vous que vos dispositifs de gestion de crise, de continuité d'activité et de PCI peuvent constituer, dans un marché concurrentiel, un avantage pour votre entreprise ?

Avez-vous un conseil à donner aux professionnels présents dans cette salle ?

Christophe SERRANO

De plus en plus, la question du plan de continuité d'activité est posée dans les appels d'offres par les grands groupes internationaux. Sans PCA robuste et éprouvé, une entreprise se met dans une situation difficile.

Je souhaite également insister sur l'aspect évolutif de l'industrie. Nous évoluons dans un domaine où de nouveaux produits apparaissent chaque jour. Les nouveaux moyens de production doivent être testés. De ce point de vue, l'audit a son importance.

François TABOUROT

Monsieur RIVIERE, pouvez-vous évoquer l'aspect stratégique et l'avantage concurrentiel liés à la maîtrise de la continuité d'activité et donner un conseil à l'auditoire ?

David RIVIERE

Je ne sais pas si nous pouvons aller jusqu'à parler d'avantage concurrentiel pour les systèmes d'information de gestion.

En revanche, pour le domaine des SI industriels, dont il a été peu question aujourd'hui, l'enjeu de la continuité de service dépasse l'avantage concurrentiel : c'est une « condition de survie » (au sens de la poursuite d'exercice des activités) car ces systèmes sont de plus en plus liés à la capacité de conduite, et surtout à la sécurité du procédé industriel qui est une priorité du Groupe.

Dans les 2 cas, je donnerai comme conseil de ne pas hésiter à travailler sur les études d'impact. Soyez convaincus de la nécessité d'investir dans ce domaine.

François TABOUROT

Madame DROGUE, la maîtrise de la continuité est-elle un avantage concurrentiel pour Safran ?

Nathalie DROGUE

Probablement. Il apparaît dans la satisfaction du client.

François TABOUROT

Quel conseil donneriez-vous aux personnes ici présentes ?

Nathalie DROGUE

L'implication des dirigeants constitue le risque majeur. Dans la théorie de la mise en place de la gestion de risques, il est souvent question d'un porte-parole unique. En réalité, il existe autant de porte-parole que de salariés. Avec internet et les GSM, nous ne sommes pas à l'abri d'un appel personnel. C'est là que des informations éventuellement critiques peuvent partir.

François TABOUROT

Monsieur NOUELLE, que pouvez-vous ajouter pour conclure cette première partie ?

Daniel NOUELLE

Une entreprise « temps réel » ne peut se passer d'un PSI. Par ailleurs, pour les activités très dépendantes des systèmes d'information, des PCA restent indispensables afin d'assurer la continuité opérationnelle en cas de défaillance grave des SI.

L'impact des incidents sur nos clients gagne de l'importance. Mettre en place ces dispositifs dans une compagnie aérienne s'avère bien évidemment indispensable.

Je terminerai par une question : un PCA peut-il être progressif ou faut-il traiter dans leur globalité l'ensemble de ses aspects ? Je peux déjà fournir un élément de réponse : j'ai l'impression qu'il est possible de bâtir un PCA progressivement.

En l'absence de moyens, le PCA peut ne pas avoir pour objectif de traiter la totalité des risques.

II) Questions

De la salle

Prévoir un PSI dès le développement d'un système informatique est-il envisageable ?

Participant

Si vous avez déjà mis en place un PSI, une application nouvelle bénéficiera des solutions de PSI. Il s'agira de la caractériser : application sensible, critique ou normale. Par la suite, en fonction de sa catégorie, elle héritera des solutions mises en place par des applications qui ont le même profil.

Le remplacement d'une application existante nécessite de déterminer son niveau de criticité avec le métier.

David RIVIERE

Pour répondre en un mot à la question : oui. Cela me semble être un jalon indispensable, au moins sur deux étapes :

- l'analyse de criticité ;
- un accord sur une architecture informatique permettant de répondre aux besoins.

Si l'application n'est pas cataloguée comme critique ou vitale, ne pas disposer de solution de secours opérationnelle disponible pour la mise en production peut ne pas être bloquant, à condition d'avoir planifié et budgété le test de la solution de secours.

Participant

Ces éléments sont d'ailleurs inscrits dans un SLA, qui est le contrat entre l'informatique et le métier.

De la salle

Qu'en est-il des risques de crise invisibles ? Je pense à Sony, qui s'est fait voler 2 millions de numéros de cartes bancaires. Ce risque paraît particulièrement difficile à couvrir, car il ne s'agit pas d'une interruption de service.

Participant

La première conséquence d'un tel risque porte sur l'image de l'entreprise qui subit le piratage. Il faut donc s'en protéger.

La mise en place de pare-feu peut limiter le risque de piratage de fichiers. Pour notre part, nous nous sommes dotés d'un système de cryptage des informations, notamment sur les PC des cadres supérieurs.

Par ailleurs, l'audit donne l'assurance que ces sujets sont correctement ou insuffisamment maîtrisés par l'entreprise. Nous avons par exemple réalisé un audit sur la protection des données secrètes.

François TABOUROT

Avec cette question, nous avons changé de paradigme. Il ne s'agit plus ici de continuité d'activité, mais de risque de fraude et d'image, c'est-à-dire de la gestion de crise.

Nathalie DROGUE

Une gestion de crise n'égale pas nécessairement un PCA. Ce sont l'implication des dirigeants et la bonne conduite qui sont examinées dans ce cas, plus que le lien avec la continuité d'activité.

François TABOUROT

Je remercie les intervenants ainsi qu'Elisabeth, à qui revient le mérite de l'organisation de cette table ronde.

Quelle analogie entre la démarche de résilience au niveau national et celle de continuité d'activité des entreprises ?

Yann JOUNOT

Préfet, Directeur de la protection et de la sécurité de l'Etat au Secrétariat Général de la Défense et de la Sécurité Nationale

Firouz MEGUEDAD

Monsieur JOUNOT, bienvenue à ce colloque. Pouvez-vous faire une analogie entre la démarche de résilience au niveau national et celle de la continuité des entreprises ?

Yann JOUNOT

Il est toujours délicat de conclure une journée à laquelle on n'a pas assisté, car le risque de contresens est important.

I) La démarche de résilience au niveau national

Je souhaite surtout vous apporter mon témoignage au titre des fonctions que j'occupe au SGDSN, service qui soutient le Premier Ministre dans la préparation de l'Etat sur tous les grands enjeux de sécurité.

Ma fonction concerne l'Etat dans sa globalité. Je suis évidemment attaché à l'objectif de résilience. En effet, il représente la solidité de la nation dans toutes ses composantes et la capacité à absorber des chocs, à résister, à surmonter une crise et à rétablir un équilibre.

Dans mes responsabilités, la continuité d'activité, notamment celle des entreprises, représente un élément de la résilience globale de l'Etat. Le concept de résilience est relativement nouveau, en tout cas en termes d'affirmation conceptuelle identifiée comme un objectif de l'action publique.

Pour l'Etat, cette exigence est exprimée dans le Livre blanc sur la défense et la sécurité nationale. Elle résulte d'une réflexion qui a été initiée en 2008 et qui a permis de prescrire des grands axes d'action de l'Etat.

Eu égard à la globalité des risques et des menaces, il s'agit de faire monter en gamme les segments permettant à l'Etat (au sens de nation) de continuer à fonctionner, y compris dans des situations de crise ou de catastrophe grave.

Je précise que c'est un axe stratégique partagé par la quasi-totalité de nos grands voisins. Sur ce concept, anglo-saxon, nous travaillons en relation étroite avec la Grande-Bretagne, les Etats-Unis, les Pays-Bas et l'Allemagne.

Il s'agit donc d'assurer la solidité globale de la nation et d'appliquer le concept de résilience, dont la continuité est une partie essentielle.

Si ce concept est nouveau, faut-il pour autant considérer qu'il faut complètement abandonner les pratiques antérieures ? Non, évidemment. Au titre de la résilience et de la continuité de nos fonctions essentielles, des éléments de solidité de la nation ont déjà été construits avec cette exigence de globalité.

Nous sommes d'abord attachés à construire et à consolider l'organisation de gestion de crise au niveau de l'Etat, en tirant parti du dispositif territorial qui a été prouvé. La colonne vertébrale

est fournie, au travers des préfets, par la présence permanente de l'Etat sur le territoire. Les préfets de départements sont les responsables de la sécurité au quotidien. Ils sont capables de mobiliser l'ensemble des acteurs au niveau local, en renforçant, au niveau territorial, le niveau zonal (intermédiaire entre le département et Paris).

En cas de crise majeure, un dispositif gouvernemental solide et robuste, pleinement interministériel, permet au Premier Ministre, en lien avec le Président de la République, de coordonner l'action du gouvernement pour assurer la réponse gouvernementale.

Après deux ans de tests, nous avons construit un dispositif de gestion de crise générique, qui s'incarne au travers d'une cellule interministérielle de crise : un dispositif qui met en présence l'ensemble des ministères impliqués dans une crise, et qui permet de partager l'information entre tous les acteurs, de réaliser en commun des analyses de situation et de proposer collégialement des lignes d'action.

Ainsi, le Premier Ministre et le Président de la République sont responsables du pilotage politique et stratégique de la crise. La capacité de gestion de crise se trouve alors enrichie. Des actions de communication et d'anticipation sont développées, pour éclairer la gestion de crise, en la projetant dans l'avenir et en l'inscrivant dans une dimension européenne et internationale.

Le propre des crises majeures tient au fait qu'elles sont intersectorielles. De ce fait, elles peuvent malheureusement impacter d'autres pays. Nous devons donc tenir compte des compétences qui existent au niveau européen. L'Europe doit pouvoir exprimer sa vision d'une crise majeure et mobiliser les instruments de politique sectorielle qui se trouvent au niveau européen pour appuyer les réponses nationales.

L'organisation de l'Etat s'effectue à tous les niveaux : local, gouvernemental et sur le périmètre européen et international. Le rôle de la SGDSN consiste également à prendre en charge la planification. Nous développons de ce point de vue une approche large : analyse de risques, veille d'anticipation et modernisation de l'architecture des plans gouvernementaux.

Depuis 2006, nous consolidons également la capacité des entreprises. Nous nous intéressons aux entreprises des secteurs d'activités dits « d'importance vitale » : les entreprises structurantes, dont le maintien en activité s'avère nécessaire en situation de crise pour assurer les fonctions vitales du pays. Il s'agit des secteurs de l'énergie, des transports, de la santé, de la communication, de la finance, etc.

En liaison avec les Ministères de tutelle de ces entreprises, nous avons construit depuis 2006 un dispositif qui identifie ces entreprises, leur impose des obligations liées à leur vulnérabilité, et identifie des points d'importance vitale. Nous nous efforçons de prioriser l'enjeu de sécurité au niveau des entreprises et de faire porter la responsabilité du maintien aux opérateurs eux-mêmes, pour que les situations vitales soient maintenues en situation de crise.

Cette action continue à se déployer. Nous en renforçons l'efficacité et nous en étendons le champ. La frontière européenne était assez peu présente dans la conception de la résilience il y a quelques années. A l'évidence, il convient de mieux la prendre en compte. Il s'agit d'une condition d'efficacité de la réponse nationale.

Avec les différents Ministères, nous avons lancé, pour le compte du Premier Ministre et du Président de la République, des chantiers prioritaires liés à la résilience. Ils s'adressent à deux catégories d'interlocuteurs.

- **Les citoyens**

  Ces derniers doivent avoir connaissance des risques et des menaces auxquels ils sont exposés pour pouvoir se protéger en cas de crise. Sur certains segments, notamment celui de la menace terroriste, nous devons développer des conseils comportementaux, pour que les citoyens acquièrent des réflexes d'autoprotection en situation de risque et ne représentent pas une entrave à l'action publique.

- **Les collectivités territoriales**
  Les fonctions publiques sont désormais réparties au profit des collectivités décentralisées. Or la capacité de ces collectivités à assurer, en situation dégradée, des missions de service public, est une condition de la continuité et de la résilience globale de la nation. Nous nous efforçons de mieux associer les collectivités territoriales, à la fois au travail de planification, aux exercices de tests et, au moment de la crise, aux dispositifs de conduite que nous organisons.

II) Mise en place de la continuité d'activité, en lien avec les entreprises

L'ensemble des acteurs doivent développer des réponses correspondant aux stratégies d'action que l'Etat souhaite conduire. Cela suppose que ces acteurs en gardent la capacité, y compris dans la durée. Ceci peut constituer une difficulté supplémentaire par rapport à des crises longues susceptibles de survenir sur le territoire national.

Eu égard à cette exigence d'action dans la durée, il existe d'ores et déjà des dispositifs liés à la continuité d'activité. Nous les avons éprouvés, notamment au moment de la gestion de la grippe A. Les entreprises les connaissent, dans des formes plus ou moins élaborées.

Cette année, nous avons décidé de développer, comme axe prioritaire fort, l'élaboration d'une méthodologie de continuité d'activité, qui s'inspirera d'ailleurs pour une large part des actions du monde de l'entreprise. Elle pourra également le compléter à certains égards. Elle sera mise à la disposition, à la fois des entreprises qui le souhaitent, mais également des administrations, notamment locales.

Nous tentons d'avancer sur la question des interdépendances, qui s'avère très délicate. Dans ma responsabilité d'assembler l'ensemble des éléments permettant une action efficace, je dois prendre en compte l'interdépendance des secteurs. De plus en plus, au travers de la planification, nous essayons de prendre en compte la dimension intersectorielle, notamment sur les grands impacts.

Dans cette démarche, il s'agit d'abord d'identifier cette interdépendance. Nous sommes en train de le faire sur les réseaux de communication à l'intérieur du périmètre de l'Etat. Il faut également déterminer la vulnérabilité des systèmes par rapport à ces interdépendances et être en mesure de bâtir des politiques de consolidation de ces systèmes. Dans cet axe, des actions de renforcement doivent être conduites.

Dans une dimension européenne, la France a impulsé une directive européenne qui identifie des grandes infrastructures européennes associées les unes aux autres, qu'il faut protéger pour éviter qu'un désastre dans un pays ait des conséquences sur le maintien de l'activité en France.

Pour nous, la continuité d'activité est un élément de la résilience. Cette discipline est indispensable au maintien en activité des structures prises isolément. Elle doit être identifiée comme une priorité pour les fonctions publiques et privées qui doivent être maintenues. Deux chantiers importants s'ouvrent à nous :

- les interdépendances ;
- le maintien dans la durée des organisations.

III) Questions

Firouz MEGUEDAD

Monsieur JOUNOT, le public ici présent est composé d'auditeurs d'entreprises tous secteurs confondus. Quels conseils leur donneriez-vous sur l'audit de PCA ou de PCI ?

Yann JOUNOT

N'étant pas un spécialiste de l'informatique, je ne peux répondre à cette question.

En conclusion de la table ronde précédente, j'ai entendu que la continuité d'activité représentait une préoccupation pour le public ici présent. Nous ne sommes pas nécessairement arrivés au bout de cette démarche.

Par ailleurs, il a été indiqué que le PCA pouvait être progressif, ce qui illustre le fait qu'il s'agit d'une démarche. Chacun doit s'interroger sur sa propre substance.

La démarche d'audit, utile, constitue un préalable. Elle permet de :

- favoriser la prise de conscience des priorités à maintenir au sein des entreprises et des organisations publiques ;
- vérifier la solidité des dispositifs existants.

De la salle

Vous avez évoqué la construction d'une méthodologie sur la continuité, qui sera mise à la disposition des collectivités territoriales et des entreprises. Sous quel délai sera-t-elle disponible ?

Yann JOUNOT

Nous souhaitons la finaliser d'ici à cet été. Etant générique, elle sera adaptable aux différents secteurs d'activité.

Firouz MEGUEDAD

Nous vous remercions. En France, la maturité du PCA date de quelques années dans certains secteurs. Elle peut être plus ou moins longue dans l'industrie ou dans le tertiaire. L'impulsion des pouvoirs publics constitue un véritable appui pour faire avancer ces sujets dans les entreprises.

Conclusion

Firouz MEGUEDAD
Présidente de séance

Ce colloque a été très dense et très riche en échanges. Je souhaite vous faire passer le message d'une personne qui se situe dans la continuité du côté opérationnel : vous autres, auditeurs, avez l'écoute des dirigeants.

Nous n'avons que peu parlé aujourd'hui de l'implication des dirigeants, des budgets et de la stratégie de continuité : ils sont pourtant clés dans la construction des dispositifs et dans les réponses apportées.

Puisque les dirigeants ont votre attention, n'hésitez pas à remonter les carences des dispositifs que vous observez, afin de faire avancer les choses, pour la sécurité des collaborateurs, pour la préservation du *business* et pour le service à nos clients.

Merci à tous et très bonne fin de journée.