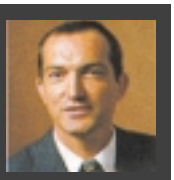
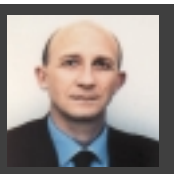
Gestion des crises

Pour un vocabulaire de crise raisonné et partagé



ALAIN DEQUIER
Risk manager
Secrétariat général de la Commission bancaire

Le règlement CRBF 2004-02 *a complété le CRBF 1997-02 relatif au contrôle interne en précisant des obligations de continuité d'activité, y compris dans les cas de chocs extrêmes. La profession bancaire doit donc parachever ses solutions dès cette année.*



PIERRE POULAIN
Chargé de mission auprès du Contrôleur général pour la prévention des riques
Banque de France

Avec la contribution des membres de la profession bancaire

LA RÉFLEXION SUR LES PLANS DE continuité d'activité fait rapidement utiliser un large vocabulaire relatif aux crises. Un glossaire sur ces termes serait appréciable. Un tel travail avait été entamé lors de la préparation au passage à l'an 2000. Il apparaît aujourd'hui que l'absence de vocabulaire commun pour décrire les rôles ou les moments lors de la traversée d'une crise pourrait être à la source de confusions qui aggraveraient la situation. Il est donc proposé dans cet article de parcourir un vocabulaire de crise en essayant de le présenter d'une manière « raisonnée » c'est-à-dire non pas sous la forme d'un glossaire, où les définitions individuelles se suivent, mais sous la forme d'un texte ordonné, où chaque terme est positionné par rapport à ses voisins, en insistant sur ce qui les distingue et en les plaçant autant que possible sur des échelles qualitative ou quantitative.

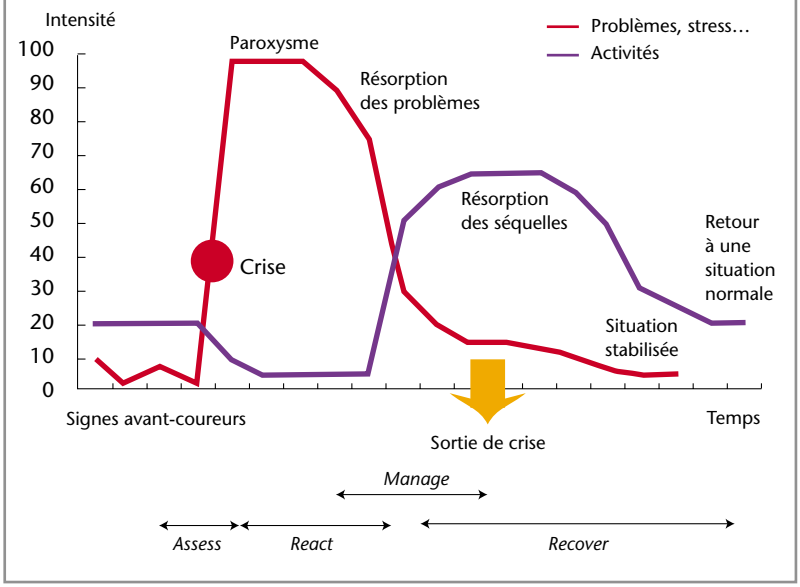
Un parallèle terminologique est aussi tenté avec le vocabulaire retenu par les *risk managers* anglo-saxons.

CHRONOLOGIE D'UNE CRISE

Sur l'échelle temporelle, il sera possible de désigner des **signes avant-coureurs** (*early warning signs/signals*) qui pourront être d'origine humaine, par exemple des menaces, des comportements anormaux… ou bien d'origine matérielle, tels des **incidents** (*events*) ou **situations d'urgence** (*emergencies situations*), pertes de données, pannes, fissures, fumées….

La **crise** (*crisis*) débute par la reconnaissance d'une situation anormale aux conséquences potentiellement très dommageables, on retiendra le terme de **sinistre** (*disaster*) lorsque ces dommages se

1. Schéma d'une crise



réalisent. Elle atteindra un **paroxysme** (*paroxysm*) au moment où la situation est la plus déstabilisée. On distinguera ensuite une **résorption des problèmes** (*damages resorption*) qui permettra de déclarer **une sortie de crise** (*end of crisis*). Celle-ci correspond à une reprise en main progressive de l'activité par les opérationnels et à une **situation stabilisée** (*stabilised situation*) qui ne présente plus de potentiel d'aggravation. Cette période n'englobe pas les conséquences de la crise qui sont facilement maîtrisables, elle est donc suivie d'une **période de résorption des séquelles** (*aftermath consequences resorption*) (retard de travail accumulé, litiges, contentieux à régler,…). Le retour à une activité régulière ne signifie pas nécessairement un retour à la situation initiale. La crise pourra, selon le cas, laisser des séquelles irréversibles ou se révéler une opportunité de progrès. On parlera de **retour à une situation normale** (*return to a normal situation*) qui permet le **rétablissement des services** (*fonctionability services*) (*schéma 1*).

Vis-à-vis de cette chronologie de crise, il faut signaler l'attitude de **vigilance** (*vigilance*) qui doit être exacerbée à l'apparition des signes avant-coureurs. Elle correspond aux mesures sécuritaires liées à la **détection** (*detection*). La vigilance peut conduire à lancer des **alertes** (*alerts*), notification formelle de la survenance d'incident, de situation d'urgence voire du sinistre lui-même. Cette information remonte la hiérarchie par **une procédure dite d'escalade** (*escalation procedure*), sa logique étant que le niveau maximum à atteindre est celui de la personne en mesure de résoudre le problème rencontré.

La remontée au plus haut niveau sollicite une **cellule de crise** (*crisis team*) composée de responsables et de spécialistes. Celle-ci va assurer le **pilotage de crise** (*crisis management*). Après la phase d'alerte et d'escalade déjà mentionnée, une phase d'évaluation ou d'**état des lieux** (*damage assessment*), ou encore d'appréciation – pour se rapprocher de l'*Assess* anglo-saxon –, doit conduire à un **point de décision** (*formal decision*) sur le choix des plans d'action à activer. Dans la réalité, ce point de décision peut se répéter au cours du temps en réaction aux événements et être vu comme une phase assimilable au *React* anglo-saxon.

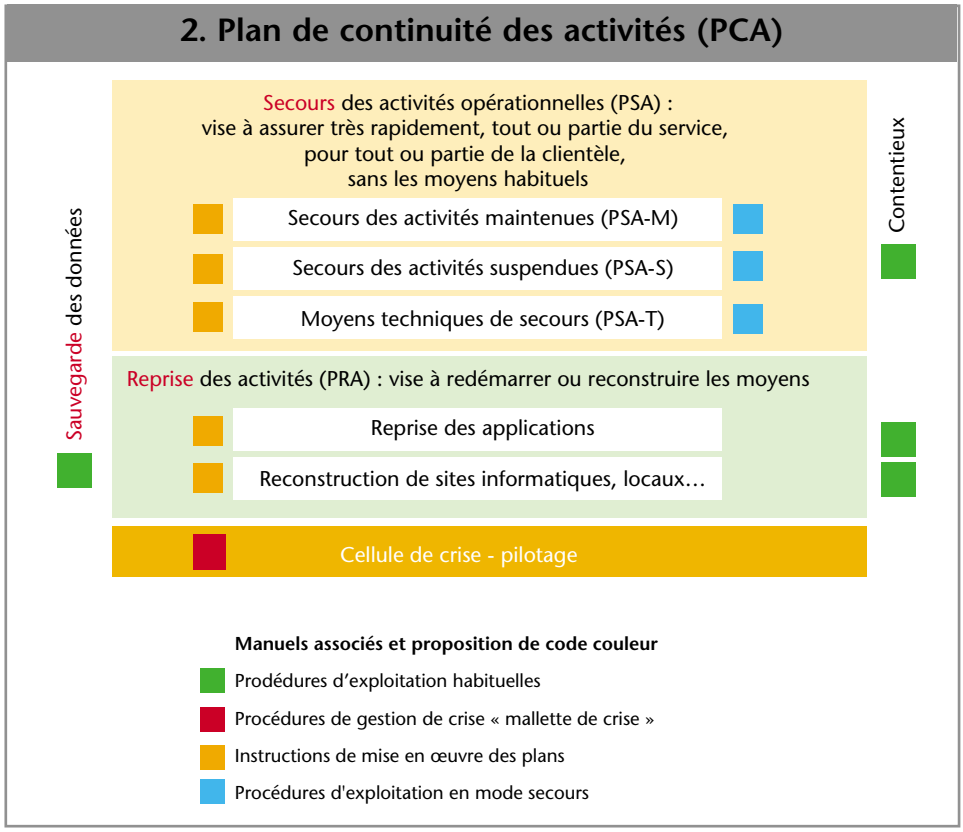
Les plans d'action décidés sont bien distincts : ceux relatifs au secours, solutions temporaires pour les activités impactées, et ceux relatifs à la reprise des activités. Leurs suivis respectifs correspondent aux deux phases anglo-saxonnes *Manage* et *Recover*. Il est proposé de retenir les termes du management (M) des secours et de la résorption (R) des problèmes, la résorption pouvant inclure celle des séquelles.

Les différentes composantes des PCA [1]

Elles peuvent être ordonnées selon l'investissement associé et l'activité résiduelle. Pour cette dernière, on distinguera le *business as usual*, donc une activité perçue sans changement pour les partenaires extérieurs – clients, fournisseurs… – et le mode dégradé avec une perte de substance. Les termes retenus seront **service normal** (*normal service*), **service dégradé** (*impaired service*).

Parmi les niveaux d'activité, nous distinguerons (*schéma 2*) :

- **le maintien grâce à des secours** (*back up*) prévus à l'avance, des hébergements sur des sites de repli, l'allocation de nouveaux espaces de travail pré-équipés… ;



• la **survie** (*survival*), l'entretien minimum des activités pour qu'elles puissent reprendre plus tard ou la **suspension** temporaire (*suspension*) ;
• voire **l'abandon** (*abandon*) de certaines activités.

A contrario, il faut noter que la crise peut générer un type d'activité qui n'est pas pratiqué en situation normale et qu'il faut anticiper.

Parmi les variantes de **reprise d'activité** (*recovery*), nous pouvons notamment citer : la **reconstruction** (*reconstruction*) de sites informatiques et/ou de bâtiments, **la reconstitution des données** (*data reconstruction*) et les **re-synchronisations de traitements** (*process re-synchronisations*).

QUELLES SONT LES CARACTÉRISTIQUES ET QUI SONT LES ACTEURS DE CES PLANS ?

Il faut d'abord signaler qu'un plan a toujours **deux facettes** (*two folds*) : l'une relative aux **métiers de la banque** (*business lines driven approach*) et l'autre aux **moyens techniques** (*technical driven approach*).

L'analyse des alertes remontées par la procédure d'escalade conduit la cellule de crise à prendre des décisions, celles-ci redescendent la hiérarchie par une **procédure de cascade** (*cascading procedure*), chaque agent ayant la responsabilité de mobiliser son niveau subalterne conformément aux plans qui ont été retenus.

L'efficacité de la gestion de crise ne peut être obtenue sans certaines actions préalables et certaines activités permanentes.

L'ensemble des activités de l'établissement doit être analysé en termes de risques et d'importance. Il s'agit de faire des cartographies de processus et des analyses de vulnérabilité. Ceci constitue la **cartographie des risques** (*risk mapping*). Les **processus d'activités sensibles** (*sensitive processes*), ceux dont la continuité est à assurer, doivent émerger de la démarche.

Les **plans de sauvegarde et restauration** (*back up and resorption plans*) des données sont aussi un préalable, ils constituent des **mesures de protection** (*protection measures*) tendant à limiter les impacts d'un sinistre.

En revanche, l'analyse des **scénarios** (*scenarios*) de sinistre constitue le cœur de la réflexion nécessaire à l'élaboration des plans de continuité d'activité, elle inclut un réexamen des priorités par rapport au fonctionnement normal en privilégiant bien entendu la préservation des vies humaines. Les différents plans définis doivent ensuite être testés régulièrement.

L'ensemble de cette gestion permanente est nommé « maintien en condition opérationnelle [2] des PCA ». L'analyse doit couvrir toute l'entreprise et être actualisée de manière périodique et « événementielle » sur tout type de modification touchant l'entreprise. Cette gestion est placée sous l'autorité d'un responsable des plans ou programmes de continuité des activités (RPCA) qui aura des correspondants dans toutes les lignes de métiers pour la création et le maintien des PCA. ■

1 PCA, plan de continuité des activités
2 MCO-PCA, équivalent du BCM, *business continuity management*, en anglais.