NORME PAS 56
Un outil pour le responsable PCA ?

Théron Paul

BCP Expert

Sarah Vignoles

Expert-conseil risque de crédit

Marouen Bellazrak

BCP Consultant

Sandra Trusty

Directeur associé

BCI France

Établie par le British Standards Institute, la norme PAS 56 est devenue une référence mondiale en matière de management de la continuité d'activité. Elle propose une méthode permettant d'atteindre la conformité avec la réglementation actuelle, mais aussi d'anticiper les durcissements inévitables de cette réglementation.

Tout encourage aujourd'hui à mettre en place des dispositifs de gestion des risques renforcés, parmi lesquels le risque de discontinuité de l'activité occupe une place déterminante pour de nombreux opérateurs, notamment dans le secteur financier. Le règlement 97-02 du Comité de réglementation bancaire et financière, traduisant les exigences posées par Bâle II, fixe une claire obligation aux établissements financiers de disposer de dispositifs de continuité coordonnés en un plan de continuité d'activité (PCA).

Peu connue encore en France, où le *business continuity management* (BCM ou management de la continuité d'activité) a encore peu de visibilité en tant que tel, la PAS 56 propose une méthode permettant d'atteindre la conformité avec la réglementation actuelle, mais aussi d'anticiper les durcissements inévitables de cette réglementation.

LA PAS 56 EXPLORE TOUS LES ASPECTS DU BCM

La norme PAS 56, inspirée des travaux du BCI et publiée par le BSI (Business Standards Institute, équivalent de l'AFNOR au Royaume-Uni, *encadré 1*), propose une démarche de mise en place d'un "système" de *business continuity management*, décrit dans PCA. Document généraliste adoptant un point de vue détaché d'un secteur d'activité ou d'un contexte particulier, il définit les principes généralement admis du BCM, décrit le processus d'implémentation du PCA (*encadré 2*) et émet des recommandations inspirées des bonnes pratiques. Ce document s'adresse donc d'abord aux porteurs de projet d'élaboration d'un PCA ou d'amélioration du dispositif de gestion du risque d'interruption de l'activité plutôt qu'aux techniciens impliqués dans la mise en œuvre concrète du processus, quel que soit leur domaine de spécialité (SI, RH...). Le processus défini par la PAS 56, comporte cinq grandes phases.

La compréhension de l'activité

La compréhension de la stratégie, de la géographie, de l'environnement et de l'activité de l'entreprise ainsi que de ses obligations et dépendances de délai et de volume de production/livraison constitue une étape fondamentale du processus. Les résultats de cette étape permettent ensuite d'étudier et de hiérarchiser les impacts de divers scénarios d'interruption et d'évaluer les risques ainsi encourus.

La stratégie de continuité

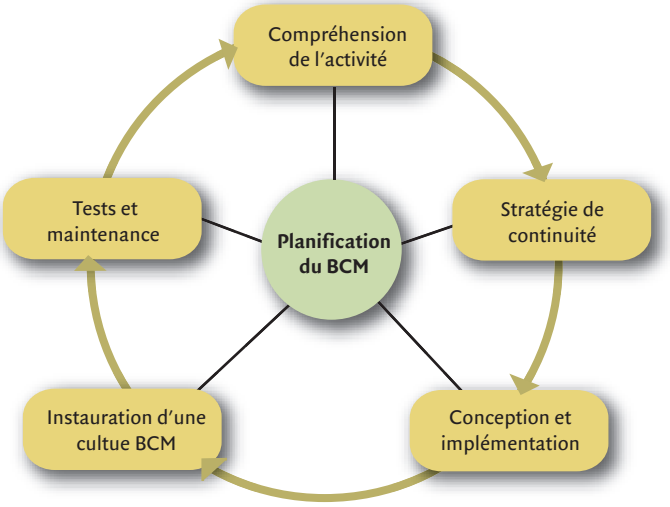
Il s'agit, dans cette deuxième étape, de définir des priorités en matière de continuité (activités vitales/

1. À L'ORIGINE DE LA PAS 56

Le Business Continuity Institute (BCI)

Le Business Continuity Institute (BCI) a été fondé en 1994 par la communauté professionnelle britannique pour permettre à ses adhérents de bénéficier de l'expérience de toute la communauté professionnelle des spécialistes de la continuité des opérations. Son schéma de certification professionnelle, organisé par niveaux de qualification, reconnaît internationalement à ses membres le statut de professionnel de la continuité des opérations. Les adhérents du BCI sont plus de 2500 aujourd'hui et se répartissent dans plus de 50 pays. Le BCI mène une action de fond au sein de la communauté professionnelle et normative en faveur de la promotion de standards méthodologiques et éthiques de haut niveau. Il est représenté, en France, par Paul Théron (www.thebci.org).

2. PCA : LA DÉMARCHE D'UN SYSTÈME DE *BUSINESS CONTINUITY MANAGEMENT*



indispensables, cibles de clientèle, territoires commerciaux, activités logistiques...) et les stratégies les mieux à même de prévenir le danger d'interruption ou de limiter les effets d'une interruption sur les périmètres ainsi identifiés comme prioritaires.

■ **La conception et l'implémentation du système de BCM**

Une fois la stratégie de continuité décidée, il faut concevoir les modes opératoires concrets qui assureront la continuité des métiers de l'entreprise (plan de continuité métier) et de ses systèmes informatiques et de communication (plan de secours informatique et télécoms). De plus, il faut prévoir l'hypothèse où l'arrêt des activités tourne à la crise [1] et, à cette fin, concevoir un plan de gestion de crise.

■ **L'instauration d'une culture BCM**

La culture est cet ensemble de croyances, de valeurs, d'attitudes et de priorités qui expliquent pourquoi les choses se font d'une certaine manière et pourquoi les individus réagissent comme ils le font dans un contexte donné. Pour développer l'intérêt des personnels pour la continuité des activités et développer des réflexes et des comportements aussi bien contrôlés que possible (ce qui est d'autant plus important si l'incident dégénère en crise), il faut bien comprendre la culture de l'entreprise et éventuellement la faire évoluer. Formation et communication institutionnelles sont des outils privilégiés de la transformation des cultures.

■ **Les tests et la maintenance**

Les réflexes ne sont acquis qu'au travers de la pratique. Afin de créer des "routines" comportementales chez les acteurs, afin de vérifier que les plans de continuité qu'on a élaborés sont opérationnels et efficaces et que toutes les ressources nécessaires seront bien disponibles et mobilisables dans les temps impartis et en état, et puis, enfin, parce que le contexte interne et externe de l'entreprise évolue sans cesse, il est indispensable de soumettre régulièrement cette dernière à des essais. Il faut tester les plans, éprouver les hommes et les ressources, et améliorer le système et les plans de management de la continuité des activités en fonction des résultats.

LE MOYEN D'ATTEINDRE LA CONFORMITÉ AVEC LA RÉGLEMENTATION CRBF

Les établissements ont l'obligation de mettre en place toutes les mesures nécessaires pour "*assurer, selon divers scénarios de crise, y compris face à des chocs extrêmes, le maintien, le cas échéant de façon temporaire selon un mode dégradé, des prestations de services essentielles de l'entreprise puis la reprise planifiée des activités*" (article 4 du règlement CRBF 97-02). En mars 2005, le CRBF a précisé ce qu'il entendait par "*prestations de services essentielles*" : toutes les "*opérations de banque et connexes ainsi que les prestations de services présentant un effet significatif sur la maîtrise des risques*".

Aux termes de l'article 14, les mesures prises doivent être coordonnées dans le cadre d'un PCA global dont la cohérence et l'efficacité doivent être régulièrement contrôlées. Les contrôles incluent, depuis mars 2005, les dispositifs mis en place chez tout prestataire concourant à la réalisation d'une prestation de services essentielle.

Le texte ne précise pas la nature des "mesures" attendues pour assurer la continuité des opérations visées. Il semble focalisé sur les mesures de réponse en cas de discontinuité matérialisée (organisation de crise, plans de secours...). Néanmoins, on ne saurait en déduire que sont exclues du périmètre les mesures de prévention et de traitement du risque de discontinuité. Ces mesures constituent évidemment le socle nécessaire pour minimiser la probabilité ou la gravité du risque. Protection des actifs critiques, formation des personnels clés, transfert à l'assurance... sont autant de solutions de premier rang pour pouvoir reprendre les activités essentielles.

UNE MÉTHODOLOGIE ORDONNÉE

Si le CRBF ne précise pas comment établir les dispositifs destinés à assurer la continuité, il suggère néanmoins une méthodologie ordonnée, résultant directement de la lettre du texte, qui établit clairement certaines étapes du processus :

- **étape 1 :** identifier les prestations de services essentielles (PSE) ;
- **étape 2 :** organiser la coordination des mesures et établir un PCA global ;
- **étape 3 :** élaborer les modes de gestion exceptionnelle et de retour à la normale ;
- **étape 4 :** établir les procédures de contrôle.

Or, pour chacune de ces étapes, et bien que cette norme soit générale et

« Il faut concevoir les modes opératoires concrets qui assureront la continuité des métiers de l'entreprise et de ses systèmes informatiques et de communication. »

[1] "Situations où, en raison de la disproportion existant entre les problèmes apparaissant et les moyens de les traiter, les organisations en charge des activités à risque se trouvent de fait dépossédées de ces problèmes par de nombreux et divers acteurs intervenant et voient leur compétence et leur légitimité remises en question (du fait, notamment, de l'intervention de la justice, etc.)", C. Gilbert, 2001. "Retours d'expérience : le poids des contraintes", Annales des Mines, Responsabilité & Environnement : Recherches débats actions. n° 22 avril 2001.

EXIGENCES DU CRBF

LA MÉTHODOLOGIE PAS 56

● Étape 1

Ce qu'exige le CRBF : identifier les prestations de service essentielles (PSE)…

Enjeu : clarifier les priorités de gestion afin de mettre en cohérence toutes les actions de gestion de la continuité. Chaque établissement établit sa liste, en partant des textes réglementaires

Principales problématiques :

- sur quels critères se fonder pour dégager puis hiérarchiser les prestations "essentielles" ?
- comment recenser les ressources nécessaires et en fixer le délai maximal d'indisponibilité ?

Ce que propose la PAS 56 :

- établit clairement quel questionnement permet d'aboutir l'identification : des "mission critical activities" (MCA), équivalentes aux PSE du CRBF ; des ressources internes ou externes nécessaires à leur exécution ; des éléments internes ou externes ayant un impact sur leur exécution ; de leurs points de faiblesse critiques
- propose deux méthodes complémentaires pour identifier les MCA/PSE, les hiérarchiser et fixer le délai maximal d'indisponibilité : analyse de l'impact de l'indisponibilité de telle ou telle activité ou business impact analysis dite BIA ; évaluation des risques susceptibles d'affecter la continuité des activités, ou risk assessment.

● Étape 2

Ce qu'exige le CRBF : organiser la coordination des mesures et établir un PCA global…

Enjeu : garantir la cohérence de toutes les actions mises en œuvre pour assurer la continuité des PSE.

Principales problématiques :

- comment avoir une vue d'ensemble de tous les besoins et réunir les différents intérêts en présence au service de l'intérêt global de l'entreprise ?
- comment assurer la maîtrise organisationnelle de tout le système mis en place ?

Ce que propose la PAS 56 : c'est par la stratégie qu'on assure la cohérence et la coordination nécessaires. La clef de voûte est la stratégie globale validée par la direction générale, faisant large part à la structure organisationnelle du dispositif. La stratégie globale se décline en stratégies spécifiques pour chaque MCA/PSE ; dans ce cas, les stratégies sont notamment fondées sur l'analyse BIA (stratégie focalisée sur les ressources nécessaires pour pouvoir assurer la continuité).

● Étape 3

Ce que qu'exige le CRBF : élaborer les modes de gestion exceptionnelle et de retour à la normale…

Enjeux : exécuter les prestations de service essentielles (procédures dégradées) ; puis restaurer le mode normal de gestion (retour à la normale, traitement des restes, etc.)

Principales problématiques :

- comment se préparer sur le plan organisationnel (management de crise) ?
- comment construire des procédures et plans utiles pour assurer la continuité en mode dégradé puis revenir à la normale (éléments fondamentaux des PCA opérationnels) ?

Ce que propose la PAS 56 : les solutions concrètes de continuité variant considérablement d'un métier à un autre, la PAS 56 recense les objectifs et éléments fondamentaux de trois types de plan :

- le plan de continuité : c'est le document de référence central, équivalent du PCA global
- le plan de ressources pour la restauration de l'activité détaille les moyens de mise en œuvre et les solutions disponibles en cas de discontinuité
- le management de crise définit l'organisation de crise et le processus de gestion de la période post-crise

● Étape 4

Ce qu'exige le CRBF : établir les procédures de contrôle…

Enjeux : évaluer la qualité des dispositifs de l'établissement et de ses prestataires ; vérifier l'efficacité des mesures, notamment en situation extrême

Problématiques :

- comment organiser un test ?
- tester un dispositif (indépendamment de la gravité du scénario) ?
- comment concilier réalisme et test sur des hypothèses de circonstances franchement exceptionnelles ?
- actualiser les données et répercuter sur le dispositif de continuité tout élément nouveau ayant une incidence sur ce dispositif.

Ce que propose la PAS 56 : une classification des exercices ainsi que les éléments sur lesquels l'exercice doit porter. Elle recense les éléments à inclure dans le processus de maintenance des dispositifs. Enfin, elle circonscrit le rôle spécifique de l'audit en matière de contrôle des dispositifs de continuité d'activité.

non spécifique aux établissements financiers, la PAS 56 apporte des réponses pratiques et utiles pour faire évoluer un dispositif existant ou élaborer ex nihilo un dispositif conforme. À l'examen de la structure de la PAS 56, sa contribution méthodologique à la mise en œuvre d'un plan de continuité d'activité au sens du CRBF est significative (*encadré 3*).

AVANTAGES ET INCONVÉNIENTS DE L'UTILISATION DE LA PAS 56

Un référentiel anglo-saxon est-il réellement adapté aux méthodes et aux pratiques à la française ? Toutefois, à cela il sera aisé d'objecter que la qualité n'a jamais tant progressé dans nos entreprises françaises que depuis que des normes internationales (ISO 9000) ont vu le jour en 1987. La question de l'origine est bien faible au regard des enjeux. Que l'on se souvienne du Livre Blanc de l'AFB sur le secours informatique qui, au milieu des années quatre-vingt-dix, dressait un panorama impressionnant du sous-équipement des établissements financiers en matière de continuité de leurs moyens informatiques. Le CRBF est une bénédiction pour les entreprises et institutions du secteur. Par ailleurs, on peut craindre une méfiance naturelle vis-à-vis d'une norme non obligatoire, quasi-inconnue sur le territoire national (les managers ont une claire préférence pour l'ISO). Mais la formation existe (et, pourquoi pas, les consultants, bien utiles dans ces moments de nouveauté…).

Enfin, la banque de demain sera soumise à des contraintes toujours croissantes en matière de gestion de ses risques. Une pression accrue que les établissements ont intérêt à anticiper en promouvant la culture adéquate et en intégrant la gestion du risque de discontinuité dans les objectifs généraux et les préoccupations quotidiennes du management. Un tel projet gagne à l'existence d'un référentiel partagé comme la PAS 56. ■