LE PLAN DE CONTINUITÉ D'ACTIVITÉ (PCA) : APPROCHE MÉTHODOLOGIQUE

Alain Coursaget et Laurent Haas

Club des Directeurs de Sécurité des Entreprises | « Sécurité et stratégie »

2014/3 18 | pages 13 à 20

ISSN 2101-4736

Le plan de continuité d'activité (PCA) : Approche méthodologique

Alain Coursaget & Laurent Haas

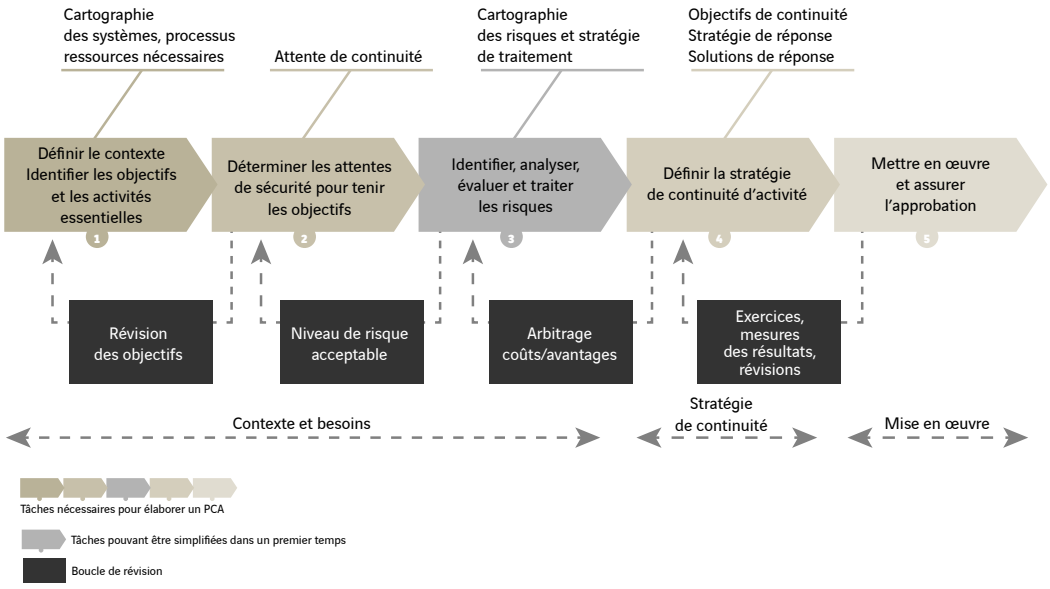
La mise en place d'un PCA est devenue une étape obligée pour toute organisation en matière de gestion de crise. Pour autant, la qualité du PCA varie considérablement d'une entreprise à l'autre. Alain Coursaget et Laurent Haas se proposent dans cet article de présenter le guide méthodologique du SGDSN (Secrétariat Général de la Défense et de la Sécurité Nationale) pour l'élaboration des plans de continuité d'activité, publié en 2014. Destinée aux organisations publiques et privées, cette publication librement accessible[1] met en cohérence les normes et approches existantes. La méthode proposée se veut simple et repose sur cinq étapes, à la fois séquentielles et itératives. La première partie vise à donner au lecteur une vision globale de l'approche méthodologique qu'il convient de suivre pour mener une démarche de continuité et de rétablissement d'activité en cohérence avec les normes. La seconde partie est constituée d'une trentaine de fiches pratiques qui décrivent de manière détaillée les étapes et visent à faciliter l'appropriation de la méthode et des bonnes pratiques en aidant leur transposition dans le contexte spécifique à chaque organisation.

Un plan de continuité d'activité (PCA) a pour objet de décliner la stratégie et l'ensemble des dispositions qui sont prévues par une organisation pour garantir la reprise et la continuité de ses activités à la suite d'un sinistre ou d'un événement perturbant gravement son fonctionnement normal. La démarche méthodologique permettant l'élaboration concrète d'un PCA est l'objet principal du guide élaboré par le SGDSN, qui a pour ambition de favoriser une telle démarche par la délivrance de conseils méthodologiques et la diffusion de bonnes pratiques. Ce document constitue également une aide à la préparation d'un éventuel projet de certification (conformité à la norme ISO 22301).

[1] *Le guide méthodologique du SGDSN pour l'élaboration des plans de continuité d'activité est librement accessible en téléchargement depuis le site du SGDSN (http://www.sgdsn.gouv.fr/site_article128.html).*

Une méthode en 5 étapes

Démarche d'élaboration d'un plan de continuité



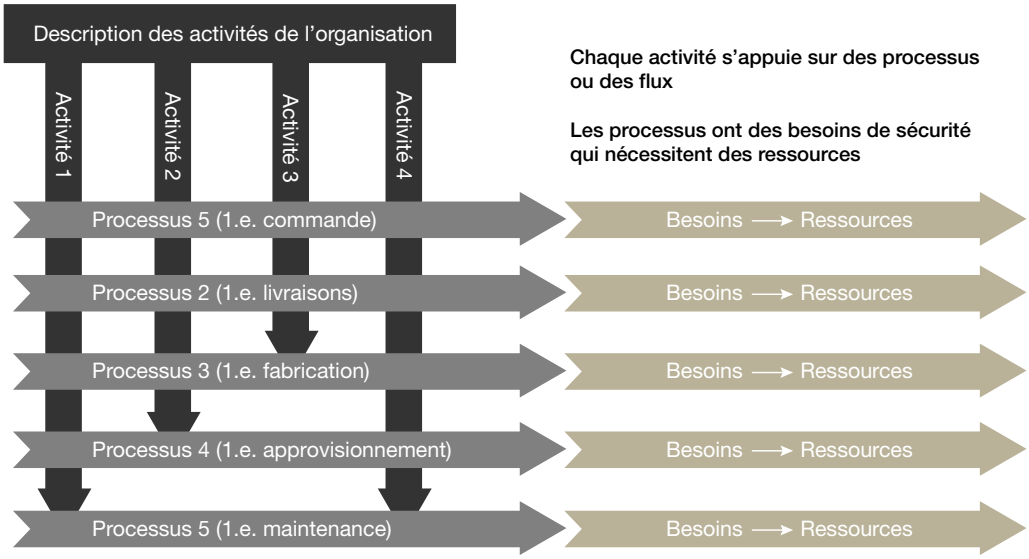
Définir le contexte, identifier les objectifs et les activités essentielles

Cette première étape est importante et conditionne l'efficacité de l'ensemble de la démarche. Elle vise à préciser le périmètre géographique et fonctionnel de l'organisation et à identifier tout ce qui peut orienter ses choix stratégiques en fonction de sa spécificité et de ses relations avec l'environnement dans lequel elle s'inscrit. L'analyse du contexte vise également à identifier les activités essentielles pour l'atteinte des objectifs de l'organisation et le respect de ses obligations. Ces activités essentielles supposent l'existence de processus et de flux (financements, matières premières, interfaces avec les systèmes d'information…) dont les plus critiques doivent être cartographiés et décrits pour la suite de la démarche.

L'analyse des activités essentielles

De ce travail doit découler une première analyse des ressources dites également « critiques » pour l'atteinte des objectifs de l'organisation (ressources humaines, infrastructures, système d'information, procédures, ressources intellectuelles et fournisseurs externes).

ACTIVITÉS ET PROCESSUS



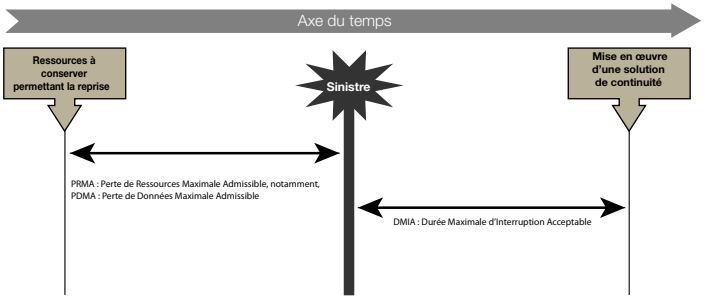
Déterminer les attentes de sécurité pour tenir les objectifs

La deuxième étape vise à préciser, pour chaque activité essentielle et chaque processus ou flux critiques, le niveau de service minimum à atteindre ainsi que la durée d'indisponibilité maximale acceptable.

Les notions clés : DMIA et PRMA

A ce stade, il est déjà possible de quantifier les conséquences d'une interruption de l'activité. Des objectifs relatifs au niveau des ressources critiques doivent être également définis. Pour simplifier le travail, l'analyse des besoins en ressources sera effectuée sur la base d'un nombre limité de scénarios (ou situations de crise) retenus comme prioritaires, à l'issue de la démarche de gestion de risque et compte tenu des besoins de continuité.

Mesurer les attentes en matière de continuité d'activité



PDMA mesure le temps maximum admissible durant lequel les données sont perdues, car elles ne peuvent pas être reconstituées; il est nécessaire de recourir aux dernières données sauvegardées.

DMIA mesure la durée d'interruption de fonctionnement du processus au-delà duquel les conséquences deviennent intolérables ; plusieurs DMIA peuvent être définis quand il y a différents modes de service dégradés (i.e. une reprise par palliers).

Identifier, analyser, évaluer et traiter les risques

Au cours de cette troisième étape, il faut concrètement :
- apprécier les différents risques, c'est-à-dire les identifier ;

-les analyser (selon les critères de probabilité et de gravité) en les intégrant à des scénarios significatifs (exemple : une crue majeure de la Seine à Paris, une pandémie grippale, une attaque informatique en déni de service...etc.) ;

-évaluer ces risques en fonction du contexte et des enjeux pour l'organisation.

Exemple de matrice pour l'évaluation des risques

Une fois appréciés et classés, les risques doivent faire l'objet d'une stratégie de traitement intégrant différentes approches (prise, refus, maîtrise, transfert, partage).

	Impacts				
Probabilité	Catastrophique 5	Majeur 4	Modéré 3	Mineur 2	Insignifiant 1
Très forte 5	10	9	8	7	6
Forte 4	9	8	7	6	5
Moyenne 3	8	7	6	5	4
Faible 2	7	6	5	4	3
Très faible 1	6	5	4	3	2

Niveau de risque encouru

9 ≤ Risque extrême ≤ 10 | 7 ≤ Risque élevé ≤ 8 | 5 ≤ Risque moyen ≤ 6 | 1 ≤ Risque faible ≤ 4

Définir la stratégie de continuité d'activité

Choisir les scénarios à prendre en compte

Les actions de prévention et de protection évoquées précédemment ont permis de réduire les risques, mais pas de les supprimer. Des risques résiduels demeurent. Ils ont une probabilité d'occurrence et peuvent conduire à une perte de ressources critiques susceptible d'entraîner une interruption d'activité au-delà du seuil acceptable, ou une diminution du niveau de service en deçà du seuil minimum prédéfini. Ces risques, constitutifs de scénarios, devront être traités dans le cadre du PCA.

Exemple de cartographie synthétique de scénarios de risques

		Impact				
		Catastrophique 5	Majeur 4	Modéré 3	Mineur 2	Insignifiant 1
Probabilité	Très fort 5					
	Fort 4	Scenario1	Scenario2 Scenario 3	Scenario 4 Scenario5		
	Moyenne 3			Scenario 6		
	Faible 2					
	Très faible 1					

Le travail de gestion des risques a permis de les caractériser en termes de vraisemblance et d'impact. Les données correspondantes seront prises en compte pour élaborer la stratégie du plan de continuité. Mais auparavant il est nécessaire de formaliser les moyens et procédures nécessaires et d'apprécier leurs coûts.

Identifier les moyens et décliner les effets à obtenir sous forme de procédures

La mise en œuvre d'un PCA repose sur des moyens identifiés et des procédures déclinées avant la survenue d'un scénario de crise. Après le sinistre, la cellule de crise pourra activer ces moyens et procédures du PCA afin de permettre une reprise partielle puis totale de l'activité. Les moyens et procédures à mettre en place couvrent en premier lieu les ressources critiques identifiées. La reprise d'activité doit par conséquent se préparer :

- en identifiant ou en créant des ressources redondantes non susceptibles d'être affectées par le sinistre ;

- en s'ouvrant la possibilité de faire appel, dans des délais adaptés, à des ressources externes ;

- en appliquant des procédures de sauvegarde des données adaptées aux exigences en termes de perte de données maximale admissible ;

- en disposant d'une organisation, d'une architecture technique et de procédures qui vont permettre le fonctionnement du centre de secours dans les délais prescrits et pour les applications prioritaires.

Prendre en compte les interdépendances pour limiter les effets en cascade

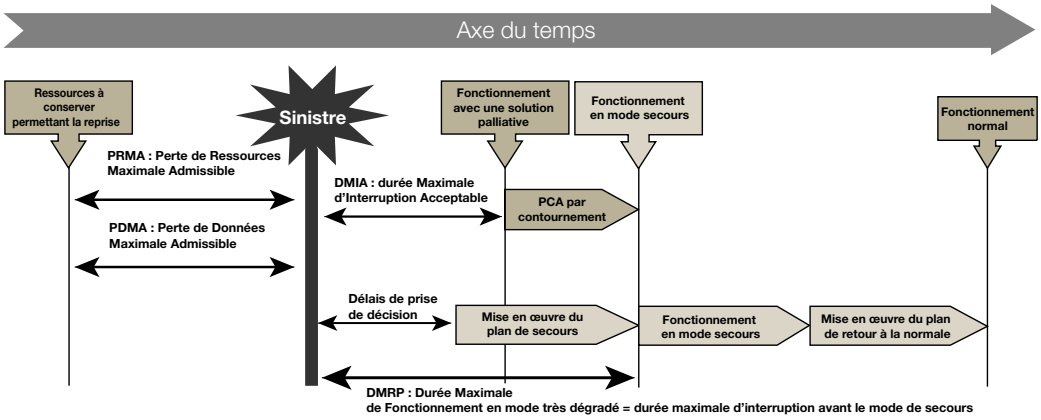
La problématique des interdépendances et des effets en cascade impose d'adopter une stratégie spécifique vis-à-vis des partenaires (prestataires et fournisseurs externes) afin de transposer les exigences internes de continuité vers l'extérieur. Ces exigences pouvant être quantifiées, l'enjeu est alors de les internaliser ou de les traduire en termes contractuels accompagnés de contrôles et de dispositifs de coordination durant une crise. Elles peuvent aussi se traduire par des mécanismes de travail en mode collaboratif avec le partage des analyses et du traitement du risque, l'élaboration coordonnée de la stratégie de continuité et la conduite d'exercices communs.

Arrêter et décliner la stratégie de continuité

La détermination de la stratégie de continuité d'activité consiste en l'identification des effets à produire et à coordonner dans l'espace et dans le temps afin de maintenir l'activité de l'organisation à un niveau prédéfini malgré l'occurrence des scénarios de risques qui ont été retenus. L'optimisation fonctionnelle de cette stratégie résulte d'une analyse comparée d'avantages et d'inconvénients. D'un point de vue économique, cette optimisation peut être caractérisée en comparant le coût de mise en place du PCA avec les bénéfices attendus (absence d'interruption d'activité au-delà du seuil défini pondéré par la probabilité de survenance, nouvelles opportunités générées par la continuité de cette activité, etc.). *(voir figure ci-contre)*

Une fois la stratégie arrêtée et déclinée en plan d'actions, les moyens à mettre en place et le dispositif de déclenchement doivent être définis afin de garantir le respect des objectifs de continuité fixés, dans le cadre du budget dédié. Les procédures associées doivent être intégrées dans les procédures de l'organisme en temps normal et durant la phase de gestion de crise.

Fixation des objectifs pour assurer la continuité d'activité



PDMA mesure le temps maximum acceptable durant laquel les données sont perdues, car elles ne peuvent pas être reconstituées ; il est nécessaire de recourir aux dernières données sauvegardées.

DMIA mesure la durée d'interruption de fonctionnement du processus au-delà duquel les conséquences deviennent intolérables.

DMRP (délais maximum de reprise technique prévu) mesure la durée d'interruption de fonctionnement des parties techniques du processus avant la reprise en mode secours. Cela correspond à la durée maximale de fonctionnement acceptable en mode très dégradé.

Mettre en œuvre et assurer l'appropriation

Mise en place du plan

Au terme des travaux décrits aux paragraphes précédents, il est possible de rédiger le plan de continuité d'activité qui va décrire la démarche logique ayant conduit au choix de la stratégie de continuité et de la réponse aux différents scénarios de crise retenus. Cette réponse consiste à préciser les moyens et à documenter les procédures qu'il conviendra de mettre en œuvre en fonction des dispositifs du PCA qui seront activés par la cellule de crise.

Les procédures spécifiques au PCA doivent être parfaitement intégrées aux procédures normales afin d'être comprises et aisément activées en situation d'urgence. Les responsables de ces moyens et procédures doivent être clairement identifiés ainsi que leur rôle et les actions attendues de leur part. La documentation doit être facilement accessible en cas de besoin et être aisément comprise. Elle doit être modifiable facilement pour permettre au PCA d'évoluer.

A ce stade il est nécessaire de s'assurer de :

-la disponibilité effective des ressources[2] ;

-la connaissance et la bonne compréhension des procédures.

Cette tâche est beaucoup plus difficile quand on s'adresse à des prestataires externes, qui ne sont pas sous le contrôle de l'organisation. Cependant, les mêmes principes doivent s'appliquer, avec, selon le cas, un contrôle direct, un contrôle documentaire, une certification par un tiers et/ou la participation à des tests ou exercices.

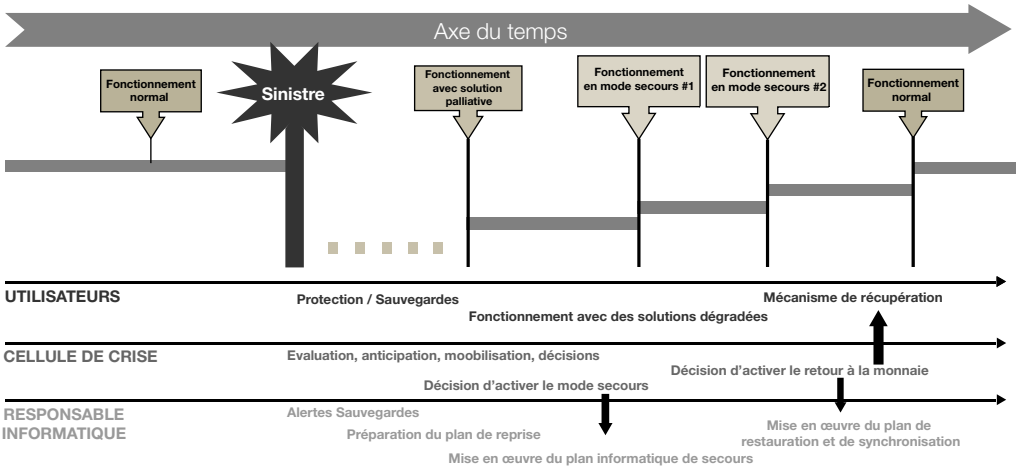
Déclenchement du plan

La cellule de crise joue un rôle clé dans l'activation des dispositifs du PCA les plus adaptés à la situation. Elle doit assurer la coordination des parties prenantes, en donnant les consignes de déclenchement des procédures préétablies et en

[2] *Il convient notamment d'être attentif au « surbooking ». Certains fournisseurs de « centre de repli » signent le même contrat avec plusieurs opérateurs, pour les mêmes ressources, mais ne peuvent les fournir qu'au « premier arrivé » lorsque l'incident survient.*

s'assurant de leur bonne mise en œuvre. *A contrario*, dans le cas d'événements fréquents, des PCA peuvent être activés en mode « réflexe », sans qu'il y ait nécessairement besoin de disposer d'une cellule de crise. Le PCA permet alors permettre de gérer l'urgence et d'éviter la crise.

Déroulement du PCA



Mesurer l'efficacité et faire évoluer le plan

Une fois que le PCA a été réalisé et que sa capacité à être mis en œuvre est garantie, il est nécessaire d'en vérifier l'efficacité. Le fonctionnement en mode dégradé et la reprise d'activité doivent se préparer en disposant de procédures testées préalablement.

La mesure de l'efficacité du PCA

Vérifier que la stratégie de continuité répond aux objectifs fixés, tels que :

- maintenir la disponibilité des activités essentielles (tenir un niveau de DMIA spécifié pour chaque activité essentielle),
- disposer d'indicateurs pour mesurer le nieau de l'activité normale et de l'activité en mode dégradé,
- protéger le patrimoine applicatif et informationnel,
- tenir la durée et le niveau de service assuré en mode d'agradé, pour chaque activité essentielle, en cas de déclenchement du plan,
- limiter la durée d'indisponibilité des activités essentielles de l'organisation et la quantité de données perdues en cas de déclenchement du plan, tant au moment de la bascule vers le site de secours qu'au retour vers le site principal,
- assurer le traitement des besoins par ordre de priorité,
- assurer le mode secours et le rétablissement selon les priorités établies,
- ne pas dépasser le coût du PCA et réduire la complexité des solutions du PCA,
- s'appuyer sur l'analyse de risque des activités et des processus de l'organisation,
- revoir cette anayse de risque en cas de découverte de nouveaux risques importants,
- améliorer la résilience en étendant progressivement les scénarios pris en compte,
- disposer d'une organisation rôdée et bien entrainée à réagir aux événements, y compris aux problèmes imprévus . . .

Différentes approches sont possibles mais en règle générale, il s'agit d'abord de faire vérifier les documents, idéalement par un « tiers de confiance », puis de tester la mise en œuvre des dispositifs (par exemple le basculement de certaines fonctions sur un site de secours), et enfin de vérifier par des exercices que les dispositifs et procédures de continuité sont connus, compris et peuvent être mis en œuvre dans les délais prescrits. Des indicateurs, tels que ceux proposés ci-dessus à titre indicatif, devront être définis et vérifiés à l'occasion d'exercices. ■

Alain Coursaget,
Directeur ACCES2S
et Laurent Haas,
Chargé de mission SGDSN

Bibliographie

Guide pour réaliser un plan de continuité d'activité, SGDSN 2013, http://www.sgdsn.gouv.fr/site_article128.html

Guide de bonnes pratiques de la Continuité d'Activité à l'attention des Directions des Ressources Humaines, Clubpca.

La sécurité économique au quotidien en 22 fiches thématiques, D2IE, avril 2014, http://www.intelligenceeconomique.gouv.fr/sites/default/files/fupload/fiches_rassemblees-v6_sansblanche.pdf

Lexique structuré de la continuité d'activité, D2IE, décembre 2012.

Livre Blanc pour la Défense et la Sécurité Nationale 2013, http://www.modernisation.gouv.fr/sites/default/files/fichiers-attaches/livre_blanc_defense-et-securite-nationale.pdf

Livre Blanc pour la Défense et la Sécurité Nationale 2008, http://www.ladocumentationfrancaise.fr/rapports-publics/084000341/

Plan de Continuité d'Activité & Gestion de Crise – Fascicule pratique de la mise en place du travail occasionnel à distance (TOAD).