GUIDE D'AUDIT

Une démarche d'audit de Plan de Continuité d'Activité (PCA)

En chinois, le mot crise, traduit par "wei-ji",
s'exprime par deux idéogrammes ;
le premier signifie danger, le second opportunité.

IFACI Institut de l'Audit Interne

DANS LA MÊME COLLECTION

- **Guide d'audit du développement durable**, Unité de Recherche IFACI
- **Contrôle interne et qualité : pour un management intégré de la performance**, Unité de Recherche IFACI
- **Des clés pour la mise en œuvre du contrôle interne**, Unité de Recherche IFACI
- **Evaluer et développer les compétences des collaborateurs**, Antenne régionale Aquitaine IFACI
- **Audit des prestations essentielles externalisées par les établissements de crédit et les entreprises d'investissement – 2ème Edition**, Groupe Professionnel «Banque »
- **La cartographie des risques**, Groupe Professionnel « Assurance »
- **L'audit interne et le management des collectivités territoriales**, Unité de Recherche IFACI
- **Cartographie des Risques**, Groupe Professionnel « Immobilier Locatif »
- **Étude du processus de management et de cartographie des risques**, Groupe Professionnel « Industrie et commerce »
- **Management des risques**, IIA UK – Traduction Unité de Recherche IFACI
- **L'auto-évaluation du contrôle interne**, Unité de Recherche IFACI
- **Une démarche de management des connaissances dans une direction d'audit interne**, Unité de Recherche IFACI
- **Pour un bon audit du dispositif de lutte contre le blanchiment des capitaux**, Groupe Professionnel « Banque »
- **L'efficacité des Comités d'audit – Les meilleures pratiques**, PwC – The IIA Research Foundation – Traduction IFACI – PwC
- **Gouvernement d'entreprise et Conseil d'administration**, PwC – The IIA Research Foundation – Traduction IFACI – PwC
- **Le rôle de l'auditeur interne dans la prévention de la fraude**, Prise de position de l'ECIIA – Traduction IFACI
- **Évaluation de la compétence dans la pratique de l'audit interne**, Prise de position de l'ECIIA – Traduction IFACI

Pour plus d'informations : www.ifaci.com

© IFACI – Paris – juillet 2008

ISBN : 978-2-915042-15-3
ISSN : 1778-7327

Toute représentation ou reproduction, intégrale ou partielle, faite sans le consentement de l'auteur, ou de ses ayants droits, ou ayants cause, est illicite (loi du 11 mars 1957, alinéa 1er de l'article 40). Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait une contrefaçon sanctionnée par les articles 425 et suivants du Code Pénal.

REMERCIEMENTS

L'IFACI tient tout particulièrement à remercier les membres de l'Unité de Recherche qui ont contribué aux différentes phases de production de ce cahier :

- Conception et rédaction :
  - **Danièle AUDAP,** *Déléguée à l'Audit, Gaz de France ;*
  - **Françoise COLLARD,** *Chef de service du Contrôle Interne, AMF ;*
  - **Michèle COPITET,** *Directrice, EGONA – CONSULTING ;*
  - **Véronique DEMACHY,** *Directrice, MICA ;*
  - **Sébastien DURIEUX (CISA, CISM, CISSP),** *Senior Manager, DELOITTE Conseil ;*
  - **Fabrice FIOUX,** *Responsable de la gestion des risques, Groupe GROUPAMA ;*
  - **Gina GULLA-MENEZ,** *Directeur Audit Processus et Projets SI, SANOFI-AVENTIS ;*
  - **Jean-Paul LEBREC,** *Manager conseil en organisation ;*
  - **Sylvie MARANGONE,** *Auditeur Interne, Groupe AGRICA ;*
  - **Michel METAYER,** *Directeur de l'Audit Interne, CASDEN Banque Populaire, Animateur de l'Unité de Recherche ;*
  - **Pierre-Henri RITHY TAN (CIA),** *Inspecteur, AMF ;*
  - **Leila ROSSANO,** *Chef de mission à l'inspection bancaire, La Banque Postale.*

- Rédaction de la fiche technique sur le plan de sécurité informatique :
  - **José BOUANICHE (CIA, CISA, CISSP),** *Auditeur interne, Caisse des Dépôts et Consignations.*

- Conseils :
  - **Unité de Recherche Informatique,** *présidée par Jean-Claude HILLION, Inspecteur général honoraire de la Banque de France.*

- Révision :
  - **Béatrice Ki-Zerbo,** *Directeur de la Recherche, IFACI.*

- Mise en forme :
  - **Julie Ferré,** *Assistante de la Recherche, IFACI.*

Louis VAURS, *Délégué Général, IFACI.*

© IFACI

SOMMAIRE

REMERCIEMENTS 3

INTRODUCTION 7

QUELQUES CLÉS DE LECTURE POUR ABORDER CE CAHIER DE RECHERCHE 9

1. CHAMP D'INTERVENTION ET CADRAGE DE LA MISSION D'AUDIT INTERNE . 11
   - 1.1. De quel type de mission d'audit s'agit-il ? 12
   - 1.2. Quel est le périmètre de la mission d'audit ? 13
   - 1.3. Comment constituer l'équipe d'audit et identifier les compétences nécessaires ? 13

2. LES NOTIONS ESSENTIELLES ASSOCIÉES AU PLAN DE CONTINUITÉ D'ACTIVITÉ 14
   - 2.1. Le PCA est un acte de gouvernement d'entreprise 14
   - 2.2. Le PCA nécessite un management opérationnel et structuré 14
     - 2.2.1. L'organisation générale 14
     - 2.2.2. Le responsable du PCA 14
     - 2.2.3. Les organes de pilotage du PCA 17
   - 2.3 Le PCA est intégré dans le système de contrôle interne de l'entreprise 18

3. LES INCONTOURNABLES DU RÉFÉRENTIEL ET DU PROGRAMME DE TRAVAIL DE L'AUDIT INTERNE 20
   - 3.1. Recueil et exploitation des informations relatives au PCA 20
   - 3.2. L'audit de la phase « Etat des lieux » du PCA 21
     - 3.2.1. De quoi parle-t-on ? 21
     - 3.2.2. Quels éléments prendre en compte dans la phase "Etat des lieux" ? 21
     - 3.2.3. Comment construire le référentiel de la mission d'audit ? 22
     - 3.2.4. Objectifs clés d'une mission d'audit pendant la phase « Etat des lieux » 23
   - 3.3. L'audit de la phase « Projet » du PCA 24
     - 3.3.1. Les principes de base 24
     - 3.3.2. Les investigations détaillées de la phase « Projet » 26

© IFACI

3.4. L'audit de la phase « Tests et validation » du PCA 29
3.4.1. Objectif général de l'audit de la phase « Tests et validation » du PCA ... 29
3.4.2. Quelle approche pour auditer la phase « Tests et validation » du PCA ? 31
3.4.3. Les éléments clés pour l'auditeur interne 35
3.5. L'audit de la phase « Maintien en condition opérationnelle » (MCO) du dossier PCA 36
3.5.1. De quoi parle-t-on ? 36
3.5.2. Les thèmes à auditer au sein de la phase MCO 37
3.5.3. Les objectifs et les principaux risques associés 42
3.5.4. Les conseils pour accompagner l'audit de la phase MCO 44

CONCLUSION 45

SIGLES ET GLOSSAIRE 47

FICHES TECHNIQUES 51

1. Recueil des informations nécessaires lors de la phase d'audit « Etat des lieux » 52
2. Guide d'audit de la phase « Projet » du PCA 57
3. Guide d'audit de la phase « Tests et Validation » du PCA 60
4. Guide d'audit de la phase « Maintien en condition opérationnelle » du PCA 63
5. Guide d'audit du Plan de Secours Informatique (PSI) 65
6. Assurance et audit de PCA 71
7. Référentiel de bonnes pratiques : communication interne, formation et PCA 73
8. Charte du PCA 76
9. « Feuille de route » du RPCA 79
10. Bilan d'impact sur activités du PCA 82
11. Questionnaire d'auto - évaluation du Plan de Continuité d'Activité (PCA) 86

BIBLIOGRAPHIE 91

© IFACI

© IFACI

INTRODUCTION

Le caractère désormais incontournable du Plan de Continuité d'Activité (PCA) est incontestable. La nécessité d'un processus de continuité d'activité dans l'entreprise est un principe primordial de gouvernance, de saine gestion. S'il est parfois favorisé par le législateur ou le régulateur voire l'exigence du client, le PCA constitue avant tout une obligation de bon sens.
Néanmoins, les acteurs d'un tel projet sont vite confrontés à une série de contraintes dont la première renvoie à l'hypothèse sous-jacente à la démarche. En effet, décider la mise en œuvre d'un plan de continuité d'activité, c'est envisager sérieusement la réalisation d'un cauchemar : la disparition de l'entreprise. Lorsque cette hypothèse extraordinaire est admise, la complexité du projet se fait vite sentir.
Le PCA a pour objet de réduire les conséquences d'événements désastreux à caractère exceptionnel et de favoriser le retour à une situation normale. Il couvre le risque d'indisponibilité partielle ou totale de l'environnement de travail. Il intègre les solutions de secours informatique. Il recoupe une stratégie de repli illustrée par des procédures métiers, organisationnelles et techniques et préalablement déterminées avec les acteurs concernés afin d'assurer la pérennité de l'entreprise, de garantir l'atteinte des objectifs stratégiques de l'entreprise et/ou de répondre à des exigences réglementaires. Cette définition rend bien compte de la complexité de la démarche liée à la diversité des processus et des parties prenantes concernés.
La conduite d'un projet PCA est probablement le seul événement qui justifie et permet de dresser un inventaire complet des processus de l'entreprise, des ressources et moyens qui leur sont nécessaires et de leur contribution aux résultats financiers. Les différents scénarios imaginés devront ramener l'impact des conséquences d'un choc majeur dans le domaine de l'acceptable et, lors du retour à une situation normale, les causes du sinistre devront être explicitées et traitées au niveau de la gestion des risques opérationnels. La cartographie des processus et des risques est entièrement mise à profit dans la mise en œuvre d'un plan de continuité d'activité.
S'agissant de la gestion des risques majeurs et du maintien des activités, le PCA contribue donc à l'atteinte des objectifs de l'entreprise. On comprend donc aisément que l'audit interne soit concerné par la mise en œuvre d'un tel projet. Ainsi, une des Modalités Pratiques d'Application (MPA) du cadre de référence des pratiques professionnelles de l'audit interne prévoit le rôle de l'audit interne dans le processus de continuité des opérations.
Par exemple, l'audit interne pourra s'assurer que la Direction Générale est informée du degré de préparation de l'entreprise à la survenance d'un sinistre. Par ailleurs, comme le PCA est un domaine où le budget peut rapidement atteindre des sommes pharaoniques, il est indispensable de justifier les coûts et d'assurer la fiabilité du suivi des dépenses. L'audit interne pourra donc donner une assurance à la Direction Générale à propos de la pertinence et de la réalité du coût des solutions envisagées et de celui de leur maintien en condition opérationnelle. En outre, le PCA fait intervenir différentes parties prenantes qui ont des objectifs et des motivations divers ; l'audit interne peut donc évaluer la réalité et l'efficience de la coordination des acteurs de chaque étape du PCA.

Quelle que soit la phase d'un projet PCA, une mission d'audit peut être programmée. La méthodologie retenue dépendra de la maturité de l'organisation dans le domaine du PCA et plus globalement en matière de contrôle interne. Dans certains cas, les auditeurs inter-

© IFACI

nes se trouvent en face de processus de continuité partiels ou inachevés, plus ou moins opérationnels et cohérents ; dans d'autres cas ils sont en face d'un terrain vague, mais dans tous les cas ils sont confrontés à des situations inattendues, des questions incongrues, des choix cornéliens et des collaborateurs souvent déroutés car peu ou pas habitués à penser à "l'impensable".
Le programme de travail de l'audit interne dépendra également du périmètre concerné (activités, localisations géographiques…).

L'ambition des contributeurs du cahier de la recherche est à l'image du sujet : IMMENSE !!! Aussi, les membres de l'unité de recherche ont-ils souhaité partager leur expérience et leur conviction quant à l'intérêt de réaliser des missions d'audit sur la continuité d'activité. Les retombées de telles missions sont tout d'abord bénéfiques pour l'entreprise mais les auditeurs internes en tirent également des bénéfices en termes de connaissances et de compétences.

© IFACI

QUELQUES CLÉS DE LECTURE POUR ABORDER CE CAHIER DE RECHERCHE

Comme toute démarche d'audit interne, l'évaluation du Plan de Continuité d'Activité s'appuie sur un référentiel de contrôle interne. Avant d'entrer dans le vif du sujet concernant la méthodologie d'audit, l'unité de recherche a donc jugé nécessaire de rappeler les fondamentaux (gouvernance, acteurs, outils …) du PCA.

S'il veut réellement apporter de la valeur ajoutée, l'auditeur interne doit avoir une connaissance suffisante du contexte et des enjeux du dossier.
Néanmoins, les connaissances nécessaires pour mener à bien une mission d'audit interne du PCA ne sont pas celles qui sont exigées des experts chargés de la mise en œuvre du plan. L'unité de recherche n'a donc pas eu pour ambition de produire un guide à destination du Responsable du Plan de Continuité d'activité (RPCA) au sein de l'entreprise. Il s'agit plutôt d'indiquer les éléments essentiels de l'élaboration, de la gestion et de la maintenance d'un PCA tout en rappelant que l'audit interne n'est pas un acteur opérationnel de la mise en œuvre du PCA.
Par ailleurs, le vocabulaire, volontairement standardisé dans l'ouvrage, doit être adapté aux fonctions, termes et sigles utilisés dans les différents secteurs professionnels.
L'unité de recherche s'est fixée comme objectif d'apporter une aide aux lecteurs pour auditer un sujet éminemment transverse, le Plan de Continuité d'Activité de l'entreprise, et déterminer le référentiel de la mission ainsi que le plan d'audit associé.

Ce cahier de la recherche est un recueil de témoignages et de bonnes pratiques. Il est le fruit des expériences et réflexions des participants amenés à travailler sur différents types de PCA, qu'il soit déclenché pour traiter un événement particulier ou qu'il soit élaboré sur des périmètres divers (Groupe, filiale, entités).

Le lecteur pourra compléter l'analyse des sujets abordés dans ce cahier en se référant à la bibliographie et notamment à d'autres publications de l'IFACI.

Ce cahier de la recherche traite de l'audit du PCA et ne se limite pas à l'audit de la gestion de crise.
En effet, la gestion d'une crise peut faire partie du PCA mais ce dernier est un processus beaucoup plus large qui intègre notamment des dispositifs de prévention de la crise et un ensemble de moyens embarqués dans la vie quotidienne de l'entreprise pour anticiper et maintenir la continuité d'activité.

Le cahier de recherche peut être utilisé de deux manières :

- soit pour auditer une phase du dossier PCA ; l'unité de recherche a identifié quatre phases :
  1. état des lieux du dossier PCA ;
  2. conduite du projet PCA ;
  3. tests et validation du PCA ;
  4. maintien en condition opérationnelle (MCO) du PCA.

© IFACI

- soit pour examiner un thème lié au PCA tel que :
  - le plan de traitement des risques opérationnels ;
  - le plan de traitement des risques informatiques ;
  - le plan de traitement des risques logistiques ;
  - la problématique des assurances (cf. fiche technique n° 6 « Assurance et audit de PCA »),
  - ….

La réflexion du groupe de travail s'est articulée autour des questions suivantes :

- De quoi parle-t-on ?
- Quelle est la démarche proposée pour construire le référentiel de la mission d'audit ?
- Comment valide-t-on les éléments construits par la mission d'audit ?
- Quels sont les éléments clés à retenir par le lecteur ?

© IFACI

1. Champ d'intervention et cadrage de la mission d'audit interne

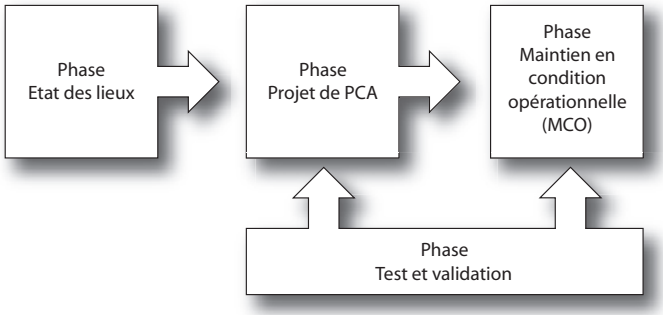
L'intervention de l'audit interne doit être préalablement cadrée et les modalités de la mission précisées. En effet, des dispositions du cadre de référence des pratiques professionnelles de l'audit interne rendent obligatoires :

- la conception et la formalisation du programme de travail de chaque mission. Ce programme précise le champ d'intervention, les objectifs, la date et la durée de la mission, ainsi que les ressources allouées (cf. norme professionnelle 2200 « planification de la mission ») ;
- la délimitation du champ de la mission « qui doit être suffisant pour répondre aux objectifs de la mission » (cf. norme professionnelle 2220 « champ de la mission »). Le périmètre d'intervention doit notamment permettre d'apprécier le niveau d'exposition aux trois familles de risques du PCA : les risques opérationnels, informatiques, et logistiques ;
- la détermination des ressources appropriées pour atteindre les objectifs de la mission. La norme 2230 préconise notamment que « la composition de l'équipe doit s'appuyer sur l'évaluation de la nature et de la complexité de la mission, des contraintes de temps et des ressources disponibles ».

En ce qui concerne le Plan de continuité d'activité, les auditeurs internes sont confrontés à l'ampleur du sujet à traiter. Les principes généraux rappelés ci-dessus s'appliquent avec encore plus d'acuité lorsqu'il s'agit de préparer une mission d'audit du PCA. Le responsable d'audit interne devra en particulier examiner :

- la séquence du projet dans laquelle se déroule la mission ;
- la nature de la mission (assurance ou conseil) ;
- le périmètre du projet ;
- le type de compétences à mobiliser.

Pour cerner la problématique du PCA, l'unité de recherche a structuré le processus en quatre phases clés illustrées dans le schéma ci-après :

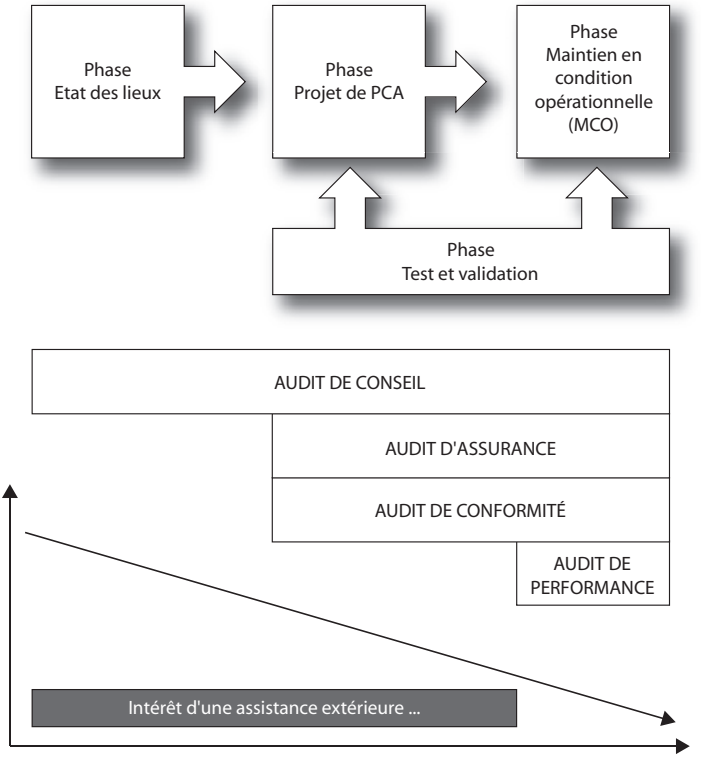


© IFACI

Le périmètre des phases n'est pas figé et doit s'adapter aux modalités organisationnelles retenues par l'entreprise pour conduire le PCA. Selon les cas, la phase « État des lieux » inclura ou non le volet lancement du projet.
On notera que la phase « Maintien en condition opérationnelle » (MCO) renvoie également à la phase « Tests et validation » lorsqu'il s'agit de qualifier les évolutions du dossier PCA et de s'assurer de la pertinence et de la fiabilité des scénarios.

1.1. De quel type de mission d'audit s'agit-il ?

L'auditeur interne devra se positionner en fonction de la mission qui lui a été confiée : s'agit-il de conduire une mission d'audit d'assurance ou de conseil sur tout ou partie du processus PCA de l'entreprise ? Par exemple, l'audit interne pourra être sollicité pour donner une assurance sur le degré de conformité de la mise en œuvre du projet par rapport aux options préalablement retenues. Il pourra également évaluer l'efficacité voire l'efficience des choix opérés par rapport aux risques identifiés.
Lors d'une mission de conseil, les auditeurs internes devront être particulièrement attentifs à ne pas remettre en cause leur objectivité et leur impartialité ; la lettre de mission devra bien préciser les attentes du donneur d'ordre.
Plus la mission d'audit se rapprochera des activités opérationnelles du PCA, plus l'aspect audit d'assurance devient prédominant comme l'illustre le graphique ci-dessous.



© IFACI

A ce stade, il convient d'insister sur le fait qu'un PCA opérationnel va au-delà du simple respect des règles émises par un régulateur ou le législateur. L'entreprise ne doit pas envisager un PCA limité à la conformité ; elle doit s'interroger plus globalement sur le maintien des activités qui ont été jugées critiques.

1.2. Quel est le périmètre de la mission d'audit ?

L'auditeur interne doit identifier :

- le domaine d'intervention : s'agit-il d'une mission d'audit sur une phase du dossier PCA ou sur une ou des thématiques associées au dossier PCA (le pilotage du dossier PCA est alors considéré comme un ensemble de preuves significatif pour le thème d'audit abordé) ?
- la couverture "géographique" de son audit (pays, …) et/ou organisationnelle (groupe, société, entreprise, site).

Le périmètre de la mission résultera d'une combinaison de ces différents facteurs.
Une bonne définition du champ d'intervention constitue un préalable pour définir les ressources nécessaires à la réalisation de la mission.

1.3. Comment constituer l'équipe d'audit et identifier les compétences nécessaires ?

La constitution d'une équipe d'audit cohérente avec les enjeux de la mission incombe au Responsable d'Audit Interne. L'identification des compétences adéquates est un des prérequis à la réussite de la mission d'audit. Les compétences nécessaires pourront évoluer au fur et à mesure de la préparation du référentiel de la mission et selon que la mission concerne :

- des activités « cœur de métier » ;
- des activités technologiques, immobilières, supports ;
- un volet « économie globale du dossier PCA » ;
- des aspects de la gestion des emplois et des compétences (profil du Responsable du PCA, complémentarité/incompatibilité des missions…)

Le cas échéant, le Responsable de l'Audit Interne pourra envisager une formation spécifique sur l'audit du PCA.
(http://www.ifaci.com/fo/seminaires/2008/audits_specifiques/audit_continuite_activites.asp)

Par ailleurs, au regard de l'expertise nécessaire sur certaines phases de l'audit PCA, le recours à un prestataire externe de services d'audit pourra être envisagé.

Ainsi, compte tenu des spécificités et de la nouveauté du processus, une attention particulière sera apportée à la constitution de l'équipe (pas d'auditeur interne débutant autonome).

© IFACI

2. Les notions essentielles associées au Plan de Continuité d'Activité

Les auditeurs internes doivent avoir un minimum de connaissances sur les aspects primordiaux du dossier PCA. Il convient en particulier de rappeler que la mise en place du processus de continuité d'activité est un acte de gouvernement d'entreprise et de management opérationnel. De plus, le PCA s'intègre dans le système de contrôle interne de l'entreprise.

2.1. Le PCA est un acte de gouvernement d'entreprise

La gouvernance définit une stratégie et une organisation susceptibles de répondre aux objectifs de l'entreprise. La continuité d'activité étant indéniablement un objectif commun à tout type d'organisation, la mise en place d'un PCA nécessite un acte de gouvernance pour intégrer la continuité d'activité dans la culture de l'entreprise et préparer l'avenir par une implication visible des organes de gouvernance.
Le gouvernement d'entreprise détermine les moyens nécessaires à la satisfaction des différentes parties prenantes en s'appuyant sur un management fort. Il tient compte des normes externes, des exigences réglementaires et des instructions internes en particulier celles de la Direction Générale.

2.2. Le PCA nécessite un management opérationnel et structuré

Le processus de continuité d'activité s'appuie sur différents acteurs et des instances de pilotage.

2.2.1. L'organisation générale

La désignation de l'ensemble des acteurs du projet PCA (Responsable du PCA, Responsable du Plan de Secours Informatique (PSI), Responsable logistique, Correspondants Continuité d'Activités, …) doit être nominative et officielle. Le rôle de chaque acteur doit être clairement défini et connu.

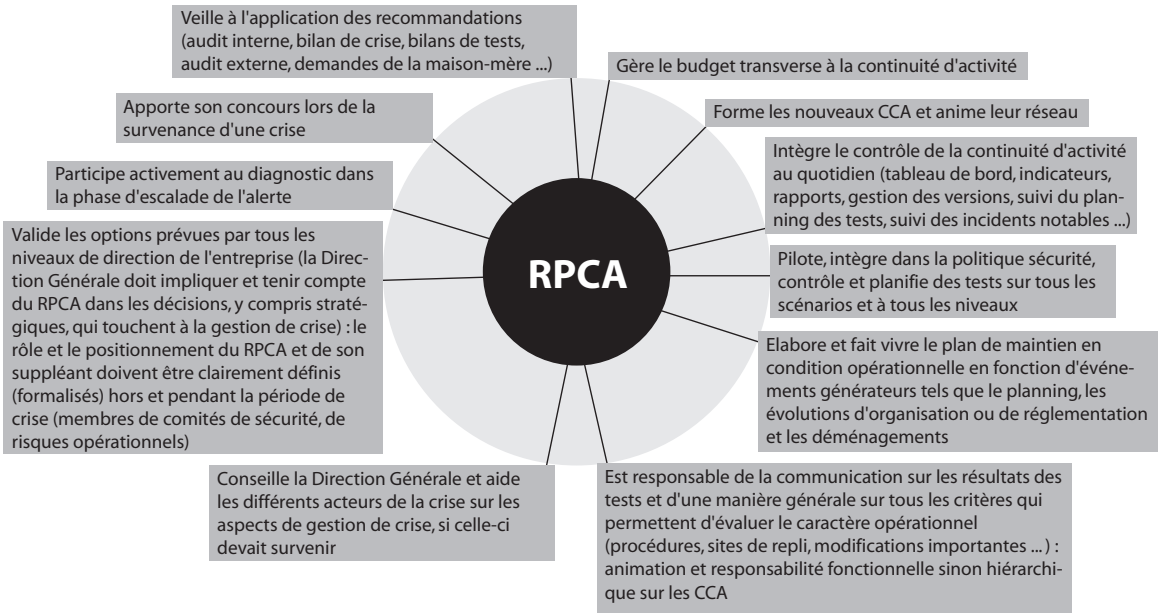
Bonne Pratique : L'auditeur interne s'attachera à obtenir les documents (fiches de fonction existantes, les lettres de mission …) définissant les rôles et responsabilités des parties prenantes du PCA.

Les fonctions en charge de la gestion des risques et des contrôles (Risk Manager, Compliance Officer, Contrôleur Interne…), doivent être associées au processus. Leur niveau d'implication dépendra de leurs compétences et de leur périmètre de responsabilités.
La délimitation des responsabilités et la clarification des rôles sont d'autant plus nécessaires lorsque les personnes désignées occupent d'autres fonctions.

© IFACI

2.2.2. *Le responsable du PCA*

Le Responsable du PCA (RPCA) est un acteur clé du processus.
Cette fonction pérenne de l'entreprise doit être reconnue et pouvoir influer au plus haut niveau sur les éléments constitutifs du plan et les décisions de l'entreprise tant pendant la gestion d'une crise qu'en situation normale.
Par conséquent, l'auditeur interne doit être vigilant sur le positionnement du RPCA. Il est également important de s'assurer de la complétude des attributions et de la permanence des activités du RPCA.
Le RPCA n'agit pas de façon solitaire ; il doit trouver des relais dans toute l'entreprise au travers des Correspondants Continuité d'Activité (CCA), installés dès la phase projet. Leur rôle ne s'arrête pas à la première période de tests probants. Le RPCA doit donc avoir les moyens d'animer un réseau en s'appuyant, entre autres, sur des indicateurs, des tableaux de bord, des plans d'actions, des métriques et des référentiels. Il prendra le soin de s'assurer de l'adéquation de ces outils avec ceux de la Direction des Risques (recensement des risques opérationnels, cartographie des risques, suivi et gestion des incidents, …) et ceux de la Direction des Systèmes d'Information (référentiels des applications, référentiels sécurité des Systèmes d'Information (SI), suivi et gestion des incidents informatiques, …).
Le schéma ci-après présente les principales attributions du RPCA, de la mise en place d'un PCA dans l'entreprise à la survenance d'une crise et à sa gestion.



Compte tenu de ces différentes attributions, le profil type du RPCA intègre des compétences telles que :

- le sens de l'organisation ;
- la capacité à animer une filière ;

© IFACI

- la compréhension des exigences réglementaires et normatives ;
- la connaissance des techniques de contrôle et de management des risques ;
- la compréhension des systèmes d'information.

L'auditeur interne s'assurera de la bonne adéquation entre le profil du RPCA, ou éventuellement de ses collaborateurs immédiats, et les pré-requis exposés ci-dessus. Il faut noter que lors des investigations, l'auditeur pourra être amené à identifier des missions, rôles et compétences proches de celles d'un RPCA : par exemple, le RSSI (Responsable de la Sécurité des Systèmes d'Information).
La désignation du RPCA et la mise en place de l'organisation doivent intervenir dès le démarrage de la phase « Projet ». Il est même souhaitable que le futur RPCA soit associé à la direction du projet dès son lancement. Il participera ainsi à la définition :

- du contour de son poste futur ;
- de l'organisation de crise qui sera mise en place ;
- de la documentation et des moyens nécessaires ;
- du processus de maintien en condition opérationnelle (MCO) en relation avec les autres processus ;
- du plan de tests et des exercices à réaliser.

Tout au long de la phase « Projet » (y compris le maintien en condition opérationnelle), le positionnement et le rattachement hiérarchique du RPCA doivent être en adéquation avec les besoins et les contraintes de l'entreprise. Sa hiérarchie devra considérer le PCA comme une priorité, intervenir pour valider le correct déroulement des phases du projet et assurer le contrôle de premier niveau du PCA.
Pour être en mesure de superviser l'ensemble du projet, le RPCA doit bénéficier d'un rattachement à même de faciliter une coordination régulière avec d'autres acteurs, notamment avec le responsable du Plan de Secours Informatique (PSI).

Le RPCA doit être indépendant de toute fonction opérationnelle et en particulier de l'informatique. Cette indépendance est définie dans une lettre de mission (éventuellement établie selon les phases du projet) ou une fiche de fonction. Idéalement, le RPCA devrait être totalement dédié à cette fonction. Néanmoins, selon la taille de l'entreprise, le RPCA peut également assumer d'autres rôles, mais en aucun cas relever de l'audit interne. Ses fonctions complémentaires peuvent être :

- secrétaire général ;
- responsable des risques ;
- responsable de la sécurité des systèmes d'information (RSSI) ;
- responsable de la logistique.

<u>Bonne Pratique</u> : Le RPCA doit avoir un rattachement et une indépendance suffisants pour faciliter la mobilisation de tous les acteurs du processus et la mise en œuvre des ressources nécessaires.
Lorsque le RPCA occupe d'autres fonctions, les auditeurs internes s'assureront de l'adéquation de ces différentes responsabilités selon les phases du PCA.

Comme mentionné ci-dessus, le RPCA travaille en constante synergie avec les acteurs du processus de continuité d'activité. En dehors des relations bilatérales qu'il peut entretenir avec les autres fonctions, le RPCA interagit avec les autres acteurs concernés à travers la participation à différents comités. Notamment, pour garantir l'homogénéité des démar-

© IFACI

ches sur les risques, le RPCA peut faire partie des comités de sécurité et des risques de l'entreprise.

Bonne Pratique : Le RPCA anime la continuité d'activité. Il doit donc être reconnu en interne et en externe comme un interlocuteur légitime et incontournable sur les problématiques de sécurité et de continuité. Il doit également :

- *être doté de moyens durables et suffisants pour assumer ses responsabilités ;*
- *être en mesure de mobiliser les moyens nécessaires aux « acteurs de la crise ».*

Enfin, le RPCA est le garant du maintien en condition opérationnelle du PCA.

2.2.3. *Les organes de pilotage du PCA*

L'organisation générale du projet et la fonction du RPCA doivent être surveillées et soutenues par les organes de pilotage du PCA tels que :

- **Le Comité de pilotage** à caractère décisionnel, peut être présidé par le maître d'ouvrage du PCA. Le président doit avoir le pouvoir de représenter la Direction Générale en ce qui concerne le PCA.
  Ce Comité est co-animé par le RPCA. Les responsables des domaines RH, Logistique, Informatique, Communication, Risques, y participent.
  Sa composition, ses pouvoirs, sa périodicité sont formalisés, son fonctionnement est réel et efficace.

- **Le Comité opérationnel** du PCA peut être présidé par le RPCA. Ce comité spécifique auquel participent les CCA (Correspondants des métiers ou, des entités) a pour rôle de piloter le processus de continuité d'activité et de préconiser des améliorations.
  Les responsables de domaines clés peuvent participer à ce comité opérationnel, de même que les responsables de solutions mises en œuvre dans le cadre du PCA.

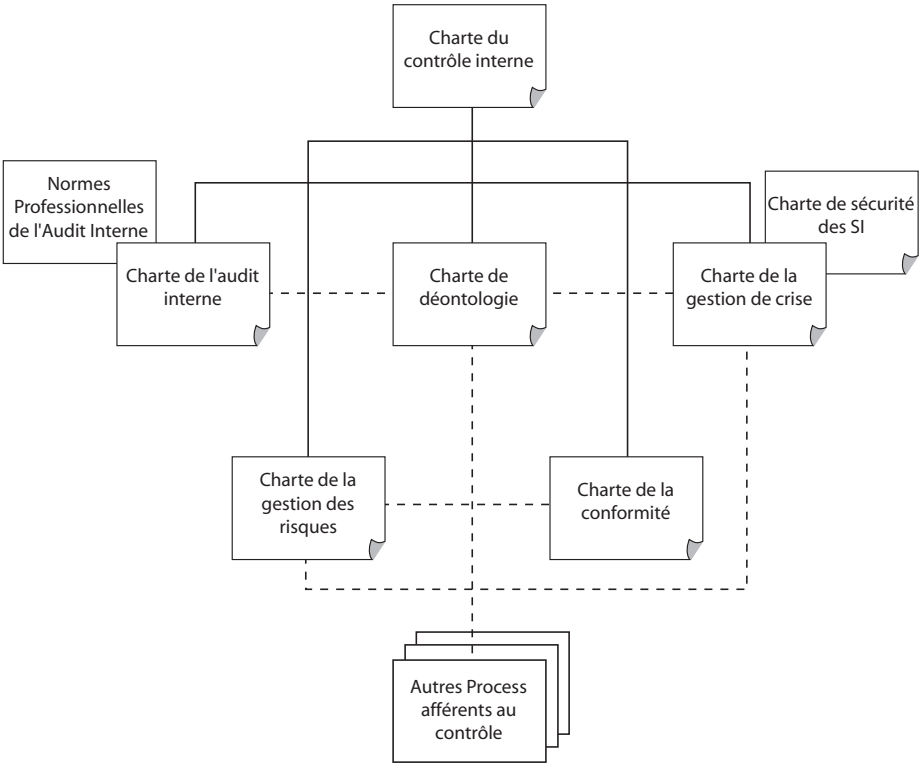
- **La cellule de crise décisionnelle (CCD) :** comme pour les autres instances, la composition, les pouvoirs, la périodicité de cette cellule sont connus. Il convient de veiller à son fonctionnement efficient, et notamment aux désignations et encadrement des cellules de crise opérationnelles (CCO).

Bonne pratique : L'auditeur interne s'assure de l'implication de la Direction Générale.
L'auditeur interne examine également le caractère efficient et non redondant de la composition de la cellule de crise décisionnelle (CCD), et vérifie que la Direction générale est effectivement représentée dans le Comité de pilotage dans la cellule de crise décisionnelle.
Le cas échéant, il constate la formalisation des niveaux de délégations de pouvoirs.

© IFACI

2.3 Le PCA est intégré dans le système de contrôle interne de l'entreprise

Quelle que soit l'entreprise, la continuité d'activité s'inscrit dans le système de contrôle interne et de maîtrise des risques.
De ce fait, la mise en place d'une charte qui décrira les diverses modalités pratiques, mais aussi de gouvernance et de contrôle, se justifie pleinement.
On trouvera un exemple de charte du PCA en fiche technique n° 8, p.76.



La charte est mise en œuvre, **dans le cadre du système de contrôle interne de l'entreprise,** pour encadrer le plan de continuité des activités et définir ses modalités pratiques de maintien en condition opérationnelle.
Elle confirme la nécessité de prendre en compte la continuité d'activité dans les nouveaux projets et développements.
Elle impose une fréquence de révision et de validation du périmètre :

- la charte est présentée aux organes de gouvernement d'entreprise qui la valident,
- la fréquence et les modalités de révision de la charte sont précisées.

Elle définit les modalités de désignation et de rattachement du RPCA.

© IFACI

Bonne pratique : Il est important d'associer le contrôle interne dès que la décision de lancer le projet de PCA est prise, pour plusieurs raisons :

- *le contrôle interne dispose d'une vision globale des sujets réglementaires traités. Il peut donc avoir un œil averti sur la manière dont le responsable du projet veut le lancer et sur l'offre faite par les prestataires (intégration dans les autres projets réglementaires, benchmarking, …) ;*
- *le contrôle interne peut être amené à préconiser des critères de choix permettant de cadrer l'appel d'offre par rapport aux besoins réglementaires et de délais et aux faiblesses relevées au travers des missions d'audit interne ;*
- *le contrôle interne devrait systématiquement être associé au pilotage du projet dans le cadre des comités de pilotage. Son avis sera un gage de conformité pour la direction du projet ;*
- *le contrôle interne doit s'assurer que le PCA est opérationnel et ainsi, entrer dès que possible un chapitre PCA dans le cadre de son plan d'audit annuel. Afin de « roder » son processus, le contrôle interne peut donc être associé à l'analyse du suivi du projet par la mise en œuvre d'indicateurs adaptés et la production de questionnaires d'analyse pendant la phase « Projet ».*

© IFACI

3. Les incontournables du référentiel et du programme de travail de l'audit interne

Quelle que soit la phase auditée, le programme de travail de la mission est conçu pour évaluer la situation de l'entreprise. Les bonnes pratiques présentées ci-après constituent des repères pour mesurer des faiblesses et proposer des pistes d'amélioration.

3.1. Recueil et exploitation des informations relatives au PCA

L'auditeur interne, une fois mandaté, collecte toutes les données nécessaires à un premier diagnostic du PCA.
Il classe ces informations selon les catégories suivantes :

- **phase du PCA :** état des lieux, projet, tests et validation, MCO ;
- **thème :** assurance, réglementation, formation, recours à des prestataires externes…
- **type d'activités :** cœur de métier, informatiques, immobilières, support…

Bonne Pratique : Quel que soit le stade d'avancement du PCA, il convient de prendre en compte les phases en amont pour :

- *avoir une vision d'ensemble et une correcte identification des causes des dysfonctionnements relevés lors d'analyses internes ou externes précédentes (commissaires aux comptes, instances de contrôle,…);*
- *vérifier la sélection des processus couverts, évaluer la cohérence avec la cartographie des risques de l'entreprise, la pertinence du montage des scénarios avec les exigences de continuité ;*
- *s'assurer de la correcte validation de la phase auditée ;*
- *préciser les conditions de cette validation et les réserves éventuelles.*

L'exploitation des informations ainsi recueillies doit permettre à l'audit interne d'identifier de manière macroscopique certains dysfonctionnements et/ou certaines zones à risques.
Ainsi doit-il s'attacher à :

- constater l'existence des livrables clés du dossier PCA et la complétude des documents ; pour cela, il pourra utilement se reporter au questionnaire d'auto-évaluation du PCA donné en fiche technique n°11, p. 86.
- évaluer la cohérence technique des documents et leur adéquation sur le plan organisationnel ; il s'agira pour l'auditeur interne d'identifier les liens entre documents, et d'analyser la cohérence des mises à jour, des décisions auxquelles ils font référence… ;
- repérer les écarts éventuels entre la cartographie des risques de l'entreprise, en vigueur au moment de la mission, et la criticité des processus repérée lors du PCA ;
- vérifier l'adéquation du PCA aux besoins de continuité exprimés ; une comparaison de la Durée Maximale d'Interruption de l'Activité (DMIA) acceptable et souhaitée par les managers opérationnels et celle retenue dans le dossier PCA, est un indicateur significatif ;
- analyser l'efficience des solutions du PCA ; l'évaluation du degré d'attente des besoins exprimés au regard de la durée maximale d'interruption de l'activité

© IFACI

rapportée au coût des ressources mobilisées est un indicateur représentatif ;
- apprécier la qualité des documents destinés aux acteurs et utilisateurs du PCA.

A partir de ces premiers éléments d'analyse, **l'auditeur interne est en mesure de :**
- **préciser éventuellement son champ d'investigation** en fonction des risques potentiels encourus et des précédents audits ;
- **définir les investigations détaillées** qu'il veut mener sur les différents thèmes du PCA et/ou phases du PCA ;
- faire un point avec le donneur d'ordre et **arrêter les travaux d'approfondissement** à mener.

3.2. L'audit de la phase « Etat des lieux » du dossier PCA

3.2.1. De quoi parle-t-on ?

Il s'agit d'auditer l'état des lieux au regard d'une démarche de Plan de Continuité d'Activité. L'audit interne est alors dans la situation où son entreprise ne dispose pas d'un PCA et s'interroge sur l'opportunité de le mettre en place ou non.
La démarche d'audit proposée s'appuie sur les exigences de l'entreprise, en vue d'assurer la continuité de ses activités critiques.

S'il s'agit d'auditer la démarche d'actualisation d'un PCA, on se reportera au chapitre Maintien en Condition Opérationnelle (MCO).
(cf. § 3.5. - L'audit de la phase « Maintien en condition opérationnelle » (MCO) du dossier PCA, p.36)

3.2.2. Quels éléments prendre en compte dans la phase « Etat des lieux » ?

L'audit de la phase « Etat des lieux » du PCA peut résulter de l'analyse de la cartographie des risques ou d'une demande expresse de la Direction Générale qui souhaite évaluer l'opportunité de lancer un projet PCA. En effet :
- la permanence de la problématique de la continuité d'activité dans la cartographie des risques de l'entreprise, particulièrement en ce qui concerne les risques opérationnels, informatiques ou logistiques, peut conduire à déclencher une mission d'audit pour préciser l'analyse de l'existant ;
- dans le contexte d'une réflexion sur la pérennité de l'entreprise, la Direction Générale peut estimer que les auditeurs internes ont acquis une bonne compréhension de l'ensemble des activités d'exploitation, des fonctions individuelles et des liens qui existent entre elles. Ceci fait de l'audit interne une ressource précieuse tout au long de l'élaboration du plan de continuité des opérations.

L'auditeur interne doit identifier le cadre de la mission. Il peut s'agir :
- d'une mission d'audit d'assurance. Auquel cas, l'objectif primordial est de valider la conformité. Ainsi, la Modalité Pratique d'Application 2110-2 prévoit que l'audit interne doit évaluer régulièrement le processus d'élaboration du Plan de continuité des opérations de l'entreprise, notamment lors de l'apparition d'une exigence régle-

© IFACI

mentaire (au stade de projet ou de décret). De même, « l'audit interne doit s'assurer que la Direction Générale est informée du degré de préparation de l'organisation à la survenance d'un sinistre » ;
- d'une mission de conseil liée à une réflexion sur l'opportunité de lancer un projet PCA.

Bonne Pratique : Quel que soit le contexte de la mission d'audit interne, il convient d'examiner le processus de gestion des incidents et de retour d'expérience (débriefing de crise…). Ces données contribuent à l'analyse préalable sur la maturité de la réflexion en matière de continuité d'activité au sein de l'entreprise.

3.2.3. Comment construire le référentiel de la mission d'audit ?

Les éléments de contexte étant clarifiés, les auditeurs internes construiront le référentiel de la mission à partir d'un certain nombre de données.

3.2.3.1. Le cadrage du périmètre du PCA

La capacité de l'entreprise à définir, mettre en œuvre et maintenir une stratégie de repli en fonction des procédures métiers, organisationnelles et techniques, dépend des localisations géographiques concernées.
Dès la phase « Etat des lieux », l'audit interne prendra en compte l'incidence de ces variables. Les auditeurs internes pourront cadrer leur mission :
- en partant de la répartition des sites d'implantation ou,
- en privilégiant une approche par processus d'activités.

Plus concrètement, le périmètre de la mission d'audit résulte de la combinaison de plusieurs critères comme :
- la maille d'analyse (Groupe, entités, filiales, sites…) ;
- les types d'opérations sélectionnées dans le PCA ;
- la localisation des activités ;
- la prise en compte ou non des prestations externes.

3.2.3.2. Les processus clés et les points de contrôle

La mission se focalisera sur des zones à risque qu'il convient d'identifier en analysant :
- les processus dont la criticité est maximale. Par exemple :
  - l'élaboration et l'arbitrage des macro-hypothèses de travail ;
  - les délégations de pouvoirs ;
  - la veille réglementaire qui devra couvrir le périmètre géographique adéquat ;
  - le contrôle de gestion (construction de la valeur ajoutée de l'entreprise) ;
  - la communication d'information (appropriation du thème PCA) ;
  - la gestion des risques.
- les risques auxquels sont exposés ces processus. On distinguera cinq catégories de risques :
  - risques stratégiques ;
  - risques opérationnels, informatiques ou logistiques ;
  - risques financiers ;
  - risques externes ;
  - risques de non-conformité.

© IFACI

- les cadres législatif, réglementaire, décisionnel, organisationnel, technique à utiliser. Selon la nature des activités couvertes par le PCA, ces exigences peuvent être générales ou spécifiques à l'entreprise.

3.2.3.3. Les informations à collecter

Un tableau permettant de classer les informations à recueillir est proposé en fiche technique n°1, p.52.

Il aborde 10 groupes de questions portant sur :

1. le résultat par activité ;
2. les lignes d'activité prioritaires ;
3. les services au client qui sont caractérisés avec des éléments tels que le chiffre d'affaires, le coût, les processus commerciaux critiques, les processus support critique, les délais, la communication, les échanges ;
4. l'analyse des risques ;
5. les systèmes d'information ;
6. les ressources ;
7. la rédaction des procédures métiers (standards, en mode d'activité normale) ;
8. les acteurs potentiels du dossier PCA ;
9. la réglementation ;
10. les éléments d'économie globale (les ordres de grandeur).

3.2.3.4 Le cas de la mission d'étude d'opportunité

Dans le cas où la Direction Générale demande une mission de conseil, l'auditeur interne veillera à répondre aux questions suivantes :

- Quelle est la nature du dossier (étude d'opportunité ? dossier pour décision d'engagement ? …)
- Quelles en sont les composantes (elles dépendent des modalités de conduite de projet mises en œuvre dans l'entreprise) ?
- Qui en sont les rédacteurs ?
- Qui en sont les destinataires pour décision ? Qui en sont les destinataires pour avis ?
- Quelles ont été les différentes étapes d'élaboration, de validation, ou de recueil d'avis de ce dossier ?
- Le périmètre, les scénarios de prise de décision sont-ils appropriés ?

Bonne Pratique : Le superviseur de la mission vérifiera la complétude du référentiel de la mission d'audit interne.

3.2.4. Objectifs clés d'une mission d'audit pendant la phase « Etat des lieux »

Les données recueillies pour la construction du référentiel sont analysées afin d'évaluer le niveau de maîtrise d'un certain nombre de risques. Les principaux objectifs d'audit sont résumés dans le tableau ci-après, qui propose également quelques bonnes pratiques :

© IFACI

Objectifs d'audit	Expositions aux risques	Bonnes pratiques
Savoir si l'entreprise s'est posée la question du besoin de PCA (veille, analyse des risques, …)	Risques stratégiques (pérennité) Risques de non-conformité Risques financiers	Importance de la définition du périmètre : la qualité des interlocuteurs dépendra du périmètre.
Analyser les actions menées pour étudier le besoin ou non de PCA	Risques stratégiques (organisation, pilotage, contrôle) Risques financiers	S'assurer de l'exhaustivité des investigations. (cf. fiche technique n°1, p.52)
Vérifier les critères retenus pour évaluer l'état des lieux	Risques opérationnels Risques financiers	S'assurer de la cohérence de ces critères avec ceux habituellement retenus par l'entreprise dans le cadre du lancement d'un projet.
Examiner l'organisation mise en place	Risques stratégiques (organisation, pilotage, contrôle) Risques opérationnels	Cette organisation doit faciliter la diffusion d'une culture de management des risques au cœur du dossier PCA.
Apprécier le processus décisionnel	Risques stratégiques (organisation, pilotage, contrôle)	Faire référence à une grille d'appréciation partagée par le management de l'entreprise. Vérifier la cohérence entre organisation et délégations de pouvoirs.
Examiner le suivi des décisions prises	Risques opérationnels	Se reporter aux composantes du Contrôle Interne et aux référentiels disponibles (COSO, cadre de référence AMF,…).

3.3. *L'audit de la phase « Projet » du PCA*

3.3.1. *Les principes de base*

La phase « Projet » démarre à la fin de la phase « Etat des lieux » et s'achève avant le début de la phase « Tests et validation ».
Dès le démarrage de la mission, les auditeurs internes veilleront à s'approprier le fondement du projet en s'interrogeant sur les raisons qui ont conduit à lancer ce chantier.
La mission d'audit pourra consister à vérifier la conformité et l'efficience de la méthodologie retenue pour développer le projet (respect des décisions validées à la fin de l'état des lieux, adéquation des ressources mobilisées par rapport aux enjeux, facilité d'intégration dans la culture d'entreprise, qualité des supports …). L'audit interne peut également inter-

© IFACI

venir dans cette phase pour donner l'assurance que le projet est suffisamment implémenté et que l'entreprise peut engager les premiers tests.

Bonne Pratique : L'auditeur interne devra examiner si l'entreprise n'a pas initié au sein d'une de ses entités, un projet PCA, sur tout ou partie de ses activités. Une telle expérience pourra être une bonne source d'information pour faire un benchmark.

3.3.1.1. Quelles sont les différentes approches de l'audit de la phase « Projet » ?

L'audit de la phase « Projet » peut concerner tout ou partie du PCA. En effet, les auditeurs internes peuvent réaliser :

- un audit détaillé de chaque PCA existant dans l'entreprise :
  a. vérifier que l'état des lieux a été fait sur la base d'une modélisation des processus et une cartographie des risques,
  b. s'assurer de la validation du scénario retenu,
  c. examiner l'allocation et la mobilisation des moyens (RPCA/budget).
- un audit de certains aspects du projet ; ce type de mission peut être initié pour s'assurer que des dysfonctionnements relevés par ailleurs (y compris dans le cadre d'une autre mission d'audit) ont été pris en compte dans le PCA.

Bonne Pratique : En tout état de cause, la lettre de mission devra fixer précisément les limites de l'audit du projet PCA.

3.3.1.2. Quels sont les acteurs à rencontrer ?

Parmi tous les acteurs d'un PCA, l'acteur majeur à auditer est le futur RPCA. Des entretiens avec tous les Correspondants Continuité d'Activité (CCA) désignés sont à prévoir, ainsi que le Responsable du Plan de Secours Informatique (RPSI) ou le Responsable du Plan de Reprise d'Activités (RPRA).
Lors des entretiens avec les différents acteurs, l'audit interne s'intéressera à leurs fiches de fonctions et recueillera des informations sur la description de leurs activités et les modalités organisationnelles.

3.3.1.3. L'audit interne doit-il être présent dans les organes de pilotage du projet PCA ?

La présence de l'audit interne dans les organes de pilotage doit être envisagée dans un but purement informatif et non décisionnel.
L'avantage qu'en retirera l'auditeur interne sera :

- d'être informé de l'évolution de la phase « Projet » au même titre que les autres membres. Il pourra éventuellement détecter des points de faiblesse à auditer ultérieurement ;
- de pouvoir juger de l'efficience du Comité de pilotage sous tous ses aspects :
  - engagement des membres,
  - qualité du pilotage par le RPCA,

© IFACI

- ordre du jour précis et documenté sur la partie technique et budgétaire,
- prises de décision et orientation clairement exprimées pour chaque point soulevé,
- respect des plans d'action décidés lors des comités précédents.

Bonne Pratique : la présence de l'audit interne dans les organes de pilotage du PCA pourrait être interprétée comme une validation au fil de l'eau des décisions prises. Dans ce cas, il est préférable de s'abstenir de participer aux réunions. Néanmoins, l'audit interne demandera à être destinataire des ordres du jour et comptes rendus pour être régulièrement informé.

3.3.2. *Les investigations détaillées de la phase « Projet »*

Pendant la phase « Projet » du PCA, les travaux d'audit consistent à vérifier :

- les conditions de démarrage du projet ;
- son déroulement ;
- la préparation de la phase « MCO », afin de vérifier que le maintien en condition opérationnelle pourra être assuré dans des conditions satisfaisantes.

3.3.2.1. Vérification des pré-requis de la phase « Projet » du PCA

Cette démarche de vérification permet d'apprécier la qualité et la complétude du cahier des charges à partir duquel la phase « Projet » a été menée.

Elle vise à s'assurer que les points suivants ont fait l'objet d'une validation par le Comité de pilotage ou la maîtrise d'ouvrage désignée pour le PCA :

1. l'organisation de crise de l'entreprise ;
2. les modalités de gestion de crise;
3. le référentiel des activités ;
4. les risques opérationnels, financiers, stratégiques et de non-conformité pris en compte pour le PCA (extrait de la cartographie des risques) ;
5. l'analyse des impacts d'un sinistre sur les activités (évaluation en euros, par type de sinistre) ;
6. l'expression des besoins de continuité par activité, par application informatique ;
7. les solutions de contournement en cas de sinistre, par type de sinistre ;
8. les dispositifs de prévention et d'assurance ;
9. le budget détaillé alloué au PCA.

Bonne Pratique : Si la phase « état des lieux » du dossier PCA a fait l'objet d'un audit, il sera utile de se procurer le rapport et vérifier que les recommandations ont été mises en œuvre. L'auditeur interne doit s'assurer de la cohérence entre le cahier des charges qui découle de la phase « Etat des lieux » et les termes de réalisation de la phase « Projet ».

© IFACI

3.3.2.2. Vérification de la conception du Plan de Secours Informatique

Lors de l'audit de la phase « Projet », un des thèmes généralement abordé concerne le PCA des Systèmes d'Information et Télécommunications (PCIT). L'auditeur analysera l'existant par référence aux meilleures pratiques dans ce domaine.
Un guide d'audit du plan de secours informatique (PSI) est proposé dans la fiche technique n° 5, p. 65. Les éléments de vocabulaire, les points de repère exposés dans cette partie permettront à chacun de bâtir le référentiel le plus adapté à l'entreprise et à la situation à auditer.
La sensibilité d'une information est notamment évaluée en termes de disponibilité, de confidentialité, d'intégrité, d'auditabilité. Ces critères permettent de définir le niveau de maîtrise des risques souhaité.

Les étapes essentielles de conception du PSI

Le module 9 du SAC (Systems Assurance and Control) Report de l'IIA répertorie les 7 étapes clés de la conception d'un PSI. Elles sont complétées par des renvois à d'autres référentiels tels que le processus DS4 « assurer un service continu » du COBIT (Control Objectives for Information and related technology).

Etapes du PSI	Actions à réaliser
Organiser et conduire le projet	- former l'équipe du plan de secours ; - mettre au point un calendrier et une planification détaillée ; - évaluer les solutions de sauvegarde et les garanties existantes.
Exécuter l'analyse d'impact sur l'organisation	- développer des critères d'analyse des applications ; - définir les priorités des applications critiques.
Déterminer des consignes de fonctionnement minimal	
Analyser les risques	- analyser les risques et classifier les ressources ; - identifier les situations de perte de ressources ; - évaluer les responsabilités de l'entreprise en interne et en externe.
Concevoir le plan	- identifier des procédures alternatives ; - concevoir des procédures de reprise et de restauration ; - attribuer les responsabilités pour l'exécution de ces procédures ; - documenter le plan ; - prévoir les processus de surveillance et d'escalade.
Tester le plan	- concevoir les tests du plan ; - exécuter les tests ; - documenter les résultats des tests ; - analyser les résultats des tests.
Mettre à jour le plan	- insérer les modifications dans les exploitations et applications existantes ; - tenir compte des changements de personnel ; - intégrer les nouvelles applications ; - identifier la fréquence des tests et coordonner les tests.

© IFACI

Les démarches méthodiques comme EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) ou MEHARI (MEthode Harmonisée d'Analyse de RIsques) peuvent être utilisées lors d'une analyse de risques à couvrir par un PSI.
Enfin, la problématique de sécurité lors des procédures d'urgence n'est pas à oublier. En effet, les mesures de sécurité habituelles, concernant notamment le contrôle d'accès physique, ont tendance à ne plus être prioritaires par rapport aux besoins de reprise en condition nominale lors d'un sinistre important. Les vols ou les déprédations d'information se font alors plus facilement.

3.3.2.3 Objectifs clés d'une mission d'audit pendant la phase « Projet » du PCA

Pour chaque catégorie d'indisponibilité (informatique, immobilier, RH …), la phase « Projet » du PCA devra comporter les étapes suivantes :

- Elaboration des plans généraux (dispositifs transverses à l'entreprise tels que RH et communication) ;
- Elaboration des plans de secours organisationnels par activité ;
- Elaboration des plans de secours techniques ;
- Conception d'un Plan de Secours Informatique ;
- Efficience de la cellule de crise ;
- Reportings périodiques ;
- Gestion des incidents.

Toutes ces étapes devront faire l'objet d'une validation formalisée de la part du comité de pilotage du projet.

Thème	Objectifs d'audit
Revue du dispositif global (élaboration et organisation des plans généraux transverses à l'entreprise tels que RH, communication,…)	Identifier l'organisation du dispositif complet des relais PCA et des organes (responsables de cellule de crise, Comité de pilotage,…).
	Valider le référentiel d'activité.
	Evaluer la procédure générale du PCA élaborée par le RPCA.
	Constater la cohérence du PCA avec la cartographie des risques opérationnels.
	S'assurer de l'existence d'un processus d'actualisation et de communication.
	Vérifier le reporting budgétaire.
	Vérifier l'existence d'éventuels contrats d'assurance en cours de négociation ou actifs.
	Identifier les activités sous traitées qui doivent être couvertes par un PCA à la charge du fournisseur.
	Vérifier le respect des obligations légales, réglementaires et professionnelles de l'employeur vis-à-vis des situations exceptionnelles.

© IFACI

Thème	Objectifs d'audit
Revue du dispositif global (élaboration et organisation des plans généraux transverses à l'entreprise tels que RH, communication,…) *(suite)*	Evaluer le dispositif d'alerte des collaborateurs.
	Vérifier le plan de formation permanent aux procédures de secours.
	S'assurer de la qualité du processus de communication externe.
Audits des plans de secours organisationnels par activité	Evaluer les procédures par métiers retenus dans le PCA.
Audits des plans de secours techniques	Vérifier la conformité par rapport à l'option retenue dans l'état des lieux.
	S'assurer de la mise en œuvre de la solution retenue.
	Contrôler la démarche de recherche des intervenants ou prestataires.
Efficience de la cellule	Evaluer la Maîtrise d'Ouvrage (MOA) chargée de décrire les activités de tests et de recettes du projet.
	Assister à la cellule de crise pour juger de l'efficience et du respect des procédures de gestion de crise.
Audit des reportings périodiques faits au Comité d'audit, aux Comités de pilotage et à toute instance décisionnelle	S'assurer de la qualité de l'information diffusée aux organes de surveillance.
Audit de la gestion des incidents	Evaluer l'efficience du dispositif récurrent en place ou en cours de mise en place, que ce soit au plan de l'organisation ou au plan informatique.

Bonne Pratique : on trouvera le guide d'audit de la phase «Projet » du PCA dans la fiche technique n° 2, p.57.

3.4. L'audit de la phase « Tests et validation » du PCA

3.4.1. Objectif général de l'audit de la phase « Tests et validation » du PCA

La réalisation d'une mission au cours de la phase « Tests et validation » donne à la Direction Générale l'assurance que les efforts financiers et organisationnels consentis pour la mise en œuvre du PCA ne sont pas vains. Les auditeurs internes vérifieront notamment l'absence de dysfonctionnements majeurs au niveau du pilotage et de la maintenance.

© IFACI

3.4.1.1. Objectifs des tests du PCA

Un PCA ne saurait être considéré comme fiable[1] s'il n'est pas régulièrement testé. La phase « Tests et validation » du PCA doit permettre de démontrer au management la capacité de l'entreprise à mettre en œuvre le PCA dans les délais impartis et selon les modalités retenues. Qu'elle soit réalisée dans le cadre d'un audit, d'un exercice ou d'une auto-évaluation, la phase de test est l'une des dispositions essentielles qui assure le maintien en condition opérationnelle du plan.
Ces tests ne se restreignent pas uniquement à l'informatique, mais doivent bien concerner l'ensemble des activités métiers de l'entreprise. Le caractère probant du champ couvert par un exercice (ou un test) ne doit pas donner lieu à contestation. L'audit interne vérifiera le processus de validation préalable du périmètre de l'exercice.
Enfin, une phase de tests (comme la phase de MCO) doit comprendre une analyse des BIA (*Business Impact Analysis* ou Bilan d'Impact sur Activités) (Cf. fiche technique n°10 sur le Bilan d'impact du PCA, p.82)
Trop souvent négligée par l'auditeur interne, l'analyse des BIA doit permettre d'apprécier l'adéquation du plan avec les activités critiques de l'entreprise. Force est de constater que la répartition des activités critiques peut évoluer d'une année sur l'autre pour des raisons multiples: repositionnement stratégique d'une activité, évolution de parts de marché... Les évolutions majeures doivent se traduire par une revue du BIA associé. Cette dernière doit être réalisée au minimum une fois par an.

Bonne Pratique :
Le service qualité de l'entreprise peut apporter une aide précieuse à l'auditeur interne dans cette phase d'analyse des BIA, dans la mesure où il est généralement en charge de la formalisation des processus. Les responsables d'activité (process owner) seront ainsi facilement identifiables.

Tester le plan de continuité d'activité permet lors de l'élaboration de la lettre de mission de :

- *confirmer l'efficacité et la pertinence des dispositifs de continuité envisagés ;*
- *s'assurer de l'intégration des changements importants (activités, produits, structure …) ;*
- *familiariser les parties prenantes (personnes intervenant dans la mise en œuvre du plan : équipes métiers, équipes informatiques, moyens généraux, prestataire…) avec leurs rôles et responsabilités ;*
- *modifier ou compléter les procédures préalablement définies et identifier les axes d'amélioration.*

Différents types de tests peuvent être réalisés, dont les plus communs sont les tests unitaires et les tests de repli :

- Le test unitaire va consister à exécuter une procédure, il peut être très spécifique. Il s'agira, par exemple, d'un test de pression médiatique destiné à entraîner la Cellule de Crise Décisionnelle (CCD) aux bonnes pratiques en termes de communication et de comportements vis-à-vis des médias.

[1] *L'auditeur interne pourra utilement se référer au questionnaire d'auto-évaluation donné en fiche technique n°11*

© IFACI

- Le test de repli des utilisateurs est essentiel. Il consiste à déplacer les catégories ciblées de salariés sur un site prévu en cas d'indisponibilité des locaux principaux. L'accès au site lui-même sera testé, ainsi que les outils mis à disposition. Avec les moyens dont ils disposent, et dans un mode dégradé, les salariés doivent être en mesure d'effectuer les tâches définies dans le PCA.

Les tests doivent être réalisés à fréquence déterminée et au minimum une fois par an. Ces tests peuvent intervenir en dehors de toute planification, notamment suite à une profonde modification de la structure de l'entreprise (acquisition, cession d'une activité, migration du SI, etc.).

Bonne Pratique : Les tests peuvent mettre en évidence l'inadéquation d'un processus de MCO. Ils visent à s'assurer que le PCA couvre bien les activités qualifiées de critique sur un périmètre donné.

3.4.1.2. Risques associés à une phase de tests insuffisante

Une entreprise qui ne donne pas une importance suffisante à la phase « Tests et validation », ou qui ne teste pas régulièrement le PCA, prend le risque de :

- s'appuyer sur des procédures ou des solutions peu ou pas opérationnelles, incomplètes ou obsolètes ;
- méconnaître des actions à réaliser par les différents acteurs, et des interactions entre les différentes entités à l'intérieur d'une même entreprise ou avec un prestataire par exemple ;
- s'exposer au non respect des exigences légales et réglementaires ;
- engager des coûts inutiles (maintien d'un dispositif inadéquat par exemple) ou ne pas optimiser l'investissement initial.

3.4.2. Quelle approche pour auditer la phase « Tests et validation » du PCA ?

Les auditeurs internes qui réalisent une mission en phase « Tests et validation » du PCA adopteront une démarche qui commence par la construction d'un référentiel facilitant les évaluations et les vérifications à conduire. La nature des travaux dépendra fortement de la stratégie de tests retenue par l'entreprise.

3.4.2.1. Comprendre la stratégie de tests de l'entreprise

La stratégie de tests décidée et mise en place par l'entreprise recouvre des données sur :

- le niveau de couverture du PCA ;
- la périodicité et la séquence des tests ;
- la méthodologie mise en œuvre.

Il s'agit tout d'abord de définir les parties du PCA qui font l'objet d'un test. Les tests peuvent en effet concerner tout ou partie des aspects techniques, logistiques, organisationnels, procéduraux du PCA.

La périodicité des tests et la logique de leur séquence sont également des éléments à prendre en compte. En d'autres termes, combien de temps faut-il pour que tous les aspects du PCA fassent l'objet de tests ? Ce délai est étroitement lié aux moyens financiers et humains alloués à la phase de tests, au caractère pluriannuel et progressif des tests, mais également à la gestion courante du PCA.

© IFACI

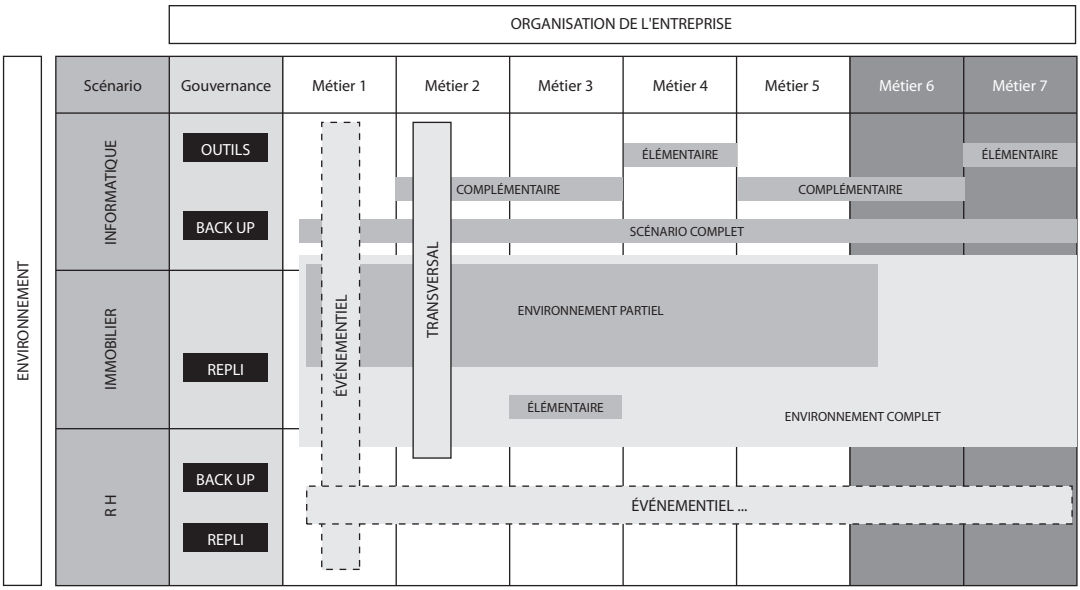
Bonne Pratique : En examinant la stratégie de tests, l'auditeur interne devra trouver dans les exercices et les tests une logique de séquence.

La prise en compte du niveau de couverture et de séquence des tests induit la typologie suivante :

- les tests élémentaires (également appelés unitaires) concernent généralement un métier au travers d'un scénario. Par exemple, le basculement d'une application informatique de l'environnement de production vers l'environnement de secours, le déplacement d'une entité sur un site de repli, la récupération et la restauration des sauvegardes externalisées.
- les tests étendus (ensemble cohérent de tests élémentaires) permettent de roder la préparation et le déroulement du PCA.
- les tests complémentaires portent sur plusieurs domaines. Ce sont, par exemple, des tests sur plusieurs systèmes informatiques (réseau, site central, échanges de données …) qui concourent à un résultat, ou sur plusieurs applications informatiques internes et partenaires (ce type de tests pourra combiner des applications avec celles qui fonctionnent en mode PCA).
- les tests de scénario complet, par exemple la totalité des applications fonctionnant sur le site de back-up, y compris les sites de back-up des partenaires ; elles sont utilisées en production normale et lors d'un retour à la normale.
- les tests transversaux ou en environnement partiel mesurent la capacité de reprise des activités critiques d'un métier ou d'une entité complète. Les tests mobilisent au moins une partie des ressources humaines concernées et touchent un ou plusieurs sites de repli. Un test « complet » associera les ressources humaines et technologiques des prestataires ou partenaires au test précédent.
- les tests événementiels simulent une situation de type pandémie ou inaccessibilité d'un local (incendie partiel, inondation …). Dans ce cas, les ressources humaines nécessaires dans la durée en fonction des BIA devront être déplacées selon les modalités prévues.

© IFACI

Cette typologie est schématisée sur la figure suivante :



Enfin, le dernier critère de qualification de la stratégie de tests porte sur la méthodologie retenue pour réaliser ces tests. Les tests peuvent être classés comme suit :

- vérification de base du plan (revue documentaire, conformité du plan…) ;
- vérification étendue du plan (analyse du contenu, des rôles et responsabilité, interdépendance…) ;
- exercice de simulation (jeux de rôle, mise en situation de la Cellule de crise décisionnelle) ;
- basculement contrôlé (test des moyens de secours sans bascule réelle, fonctionnement en parallèle) ;
- bascule réelle (test complet d'un scénario, par exemple, relocalisation d'un immeuble sur un périmètre spécifique).

Les personnes impliquées dans le déroulement des exercices peuvent avoir été préalablement informées de la date de réalisation du test, ou au contraire l'ignorer totalement. En analysant les résultats d'un test, l'audit interne doit prendre en considération l'existence d'une information préalable ou non des personnes impliquées dans l'exécution des tests. Quel que soit le type de test retenu par l'entreprise, il est communément admis qu'il doit être réalisé dans une fenêtre de temps occasionnant un minimum de perturbation pour les activités habituelles.

<u>Bonne Pratique</u> : Comprendre la stratégie de tests passe par un contrôle de conformité vis-à-vis des scénarios de risques retenus dans le cadre du PCA (couverture, adéquation aux besoins, logique de séquence, allocation budgétaire…).
Le périmètre doit intégrer la planification et le déroulement des tests chez les partenaires.

© IFACI

3.4.2.2. Construire un référentiel d'audit et identifier les techniques d'audit

Elaborer un référentiel d'audit pour la phase « Tests et validation » du PCA consiste à identifier les exigences délibérées ou réglementaires de continuité et à tester la capacité du PCA à couvrir ces objectifs.
Le matériau de base pour la construction d'un tel référentiel est donc la politique de continuité d'activité de l'entreprise. Il est également préconisé de s'appuyer sur les normes et bonnes pratiques communément reconnues dans le domaine du PCA, par exemple :

- BS 25999 part 1: « Business Continuity Management – Code of pratice » : code de bonnes pratiques pour la gestion de la continuité métier publié par le British Standard Institute ;
- ITIL (Information Technology Infrastructure Library) : bonnes pratiques en matière de gestion des services liés aux technologies de l'information ;
- GTAG-10 (Global Technology Audit Guide) de l'IIA « Business Continuity Management » ;
- autres normes tertiaires ou industrielles…

Les techniques d'audit à mobiliser sont :

- l'analyse documentaire :
  - les rapports des audits précédents ;
  - les documents d'organisation de tests du PCA ;
  - les BIA et/ou les rapports de synthèse des BIA ;
  - le plan de tests de l'année en cours et celui de l'année passée ;
  - le plan de tests de l'année suivante et éventuellement le pluriannuel ;
  - les comptes-rendus des tests récents et d'exercices ;
  - les comptes-rendus de réunion de cellule de crise ;
  - les plans d'actions qui en découlent et leur suivi ;
  - les suivis budgétaires et/ou les évaluations budgétaires.
- les entretiens avec :
  - le management ;
  - le Responsable du Plan de Continuité d'Activité (RPCA) ;
  - le service en charge des risques (Risk Manager, Responsable de la Sécurité des SI) ;
  - le(s) métier(s) ;
  - le service en charge de la définition des processus (Etudes, Normes et Méthode, Organisation Générale …) ou service qualité ;
  - les propriétaires de processus (Process Owner) ;
  - les fonctions supports (moyens généraux, SI, RH…).
- une participation en qualité d'observateur à un test (exercice de simulation par exemple). Cette méthode permet de juger la faisabilité et la pertinence des plans de tests ainsi que de la complétude de la couverture annoncée.

<u>Bonne Pratique</u> : L'auditeur interne devra faire preuve d'imagination pour collecter les éléments de preuve. Ainsi, sous réserve d'un accord préalable, l'utilisation d'appareil photo peut être utile pour étayer des constats.

© IFACI

3.4.2.3. Evaluer et vérifier

Le programme de travail de la mission d'audit est conçu pour s'assurer que :

- des tests sont planifiés et effectués régulièrement ;
- les planifications sont respectées ;
- les plans d'actions précédents ont été mis en œuvre ;
- les scénarios de tests sont réalistes (durée, localisation, ressources, coût/objectifs) ;
- chaque test est a minima défini par :
  - ses objectifs ;
  - son périmètre (les tests concernent l'ensemble des parties prenantes : filiales ou autres unités de production du groupe, sites distants, sous-traitants, co-traitants, partenaires…) ;
  - un scénario d'exécution ;
  - les participants ;
  - les critères de mesures.
- chaque exercice a fait l'objet d'un débriefing, d'un plan d'action avec des dates de mise en œuvre des recommandations et des responsables ;
- les résultats des tests ont été transmis au management et à la Cellule de Crise Décisionnelle (CCD). Ces résultats révèlent, le cas échéant, les besoins de modification du PCA.

3.4.3. Les éléments clés pour l'auditeur interne

La présence de l'auditeur interne, en qualité d'observateur, lors des exercices de simulation, mais également une visite des sites de repli ou de secours ainsi que des salles de crise, sont autant de bonnes pratiques.
L'auditeur interne ne peut donc pas se limiter à un audit documentaire, mais doit se rendre « sur le terrain » afin d'apprécier le caractère opérationnel du plan.
L'expérience montre que les exercices de simulation permettent de façon très concrète d'identifier les « points faibles » à corriger pour engager les améliorations souhaitables du plan et de l'organisation de crise.
L'auditeur s'intéressera aux hypothèses de travail du management quant aux modalités de réalisation des campagnes de tests.
La vérification de la mise en œuvre des améliorations interviendra dans le cadre du suivi de la mission d'audit interne.
Il conviendra notamment de s'assurer que l'analyse des BIA a bien été effectuée et, éventuellement, que des tests de confirmation ont été planifiés.

Bonne Pratique : On trouvera le guide d'audit de la phase « Tests et validation » du PCA dans la fiche technique n° 3, p.60.

© IFACI

3.5. L'audit de la phase « Maintien en condition opérationnelle » (MCO) du dossier PCA

3.5.1. De quoi parle-t-on ?

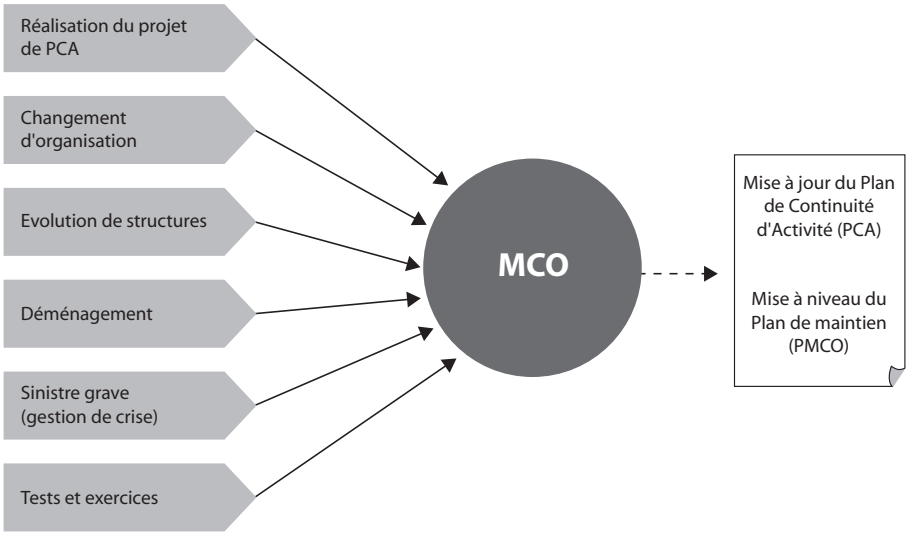
Le passage en phase MCO représente le moment où le projet est terminé. Il prend alors sa place dans les fonctions opérationnelles et entre dans une phase de mise à jour, assortie de tests réguliers. Certains standards tels que l'ITIL considèrent la continuité d'activité comme un processus d'entreprise à part entière.
La préparation du passage en phase MCO ne se réalise pas en fin de projet. Il s'organise au fur et à mesure que les éléments sont validés et diffusés par la direction du projet et le RPCA.
Ce passage se prépare dès la phase « Projet » : l'organisation de crise, la gestion documentaire du plan, la définition d'un responsable, les contrôles des évolutions, les métriques et les moyens doivent être définis pendant la mise en œuvre du projet. Ces éléments doivent avoir été corroborés, notamment dans la phase « Tests et validation ».
Tous ces critères sont exposés de façon détaillée à la Cellule de Crise Décisionnelle (CCD), ou ce qui en tient lieu dans l'organisation de l'entreprise, et validés par celle-ci.
Le passage du PCA en phase MCO doit être décidé par la direction du projet et validé par le RPCA. Il ne doit pas résulter d'un « consensus mou » ou d'une situation acquise par lassitude !

Bonne Pratique : L'auditeur interne vérifiera la formalisation du passage en MCO et appréciera les modalités de cette prise de décision ainsi que sa communication aux différents acteurs du contrôle interne. Rappelons que la validation des éléments du projet se fonde sur plusieurs méthodes complémentaires :

- *la validation documentaire ;*
- *les tests techniques ;*
- *les exercices utilisateurs.*

Gérer le MCO est avant tout un acte de gouvernement d'entreprise, qui s'inscrit dans une double perspective : l'implication interne et le lien avec l'externe. On notera que la communication dans le PCA est un des facteurs clés de sa réussite (cf. la fiche technique n° 7, p.73).
La première année de MCO est le vrai début de l'histoire du PCA et de son intégration dans une série de processus critiques (ou essentiels) identifiés comme tels dans la vie de l'entreprise.
L'organisation du PCA en scénarios, plans et thèmes, simplifie la conception modulaire des référentiels d'audit en mode MCO.

© IFACI



Cette phase n'est pas seulement le résultat de l'aboutissement du projet. Elle doit répondre elle-même à des critères conçus dans la phase « Projet » et corroborés, entre autre, par la phase « Tests et validation ».

La phase « MCO » est constituée de deux volets :

- le pilotage et la gestion des plans métiers et transversaux ;
- l'organisation des tests et exercices.

L'auditeur interne devra s'assurer de l'efficience individuelle et de la mise en cohérence de ces deux processus.

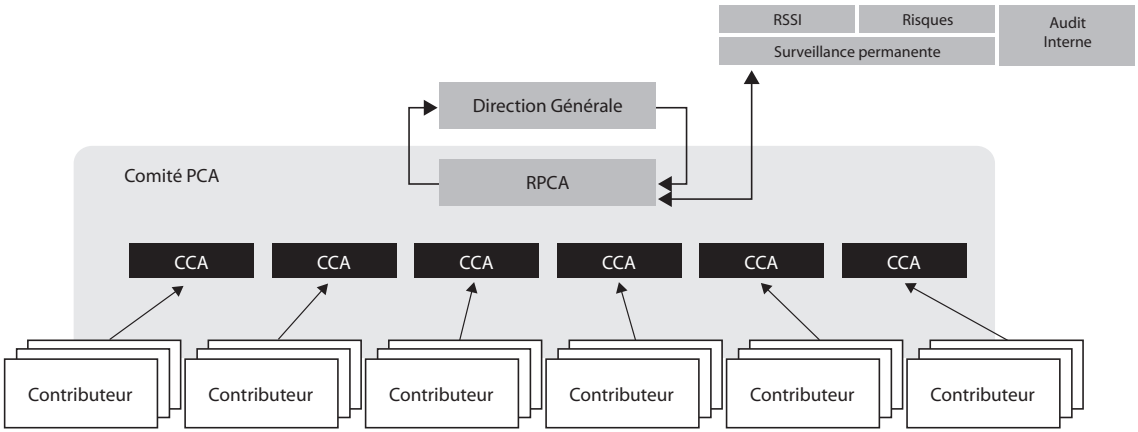
<u>Bonne Pratique</u> : Quelle que soit la taille de l'entreprise, le Maintien en Condition Opérationnelle doit comporter tous les éléments cités ci-après et justifier d'un contrôle permanent et d'audits réguliers.

3.5.2. Les thèmes à auditer au sein de la phase « MCO »

3.5.2.1. L'organisation de la phase « MCO »

L'organisation présentée ci-après allie les structures de management du PCA et les services opérationnels (cœurs de métier et fonctions support), ce qui permet d'avoir un contrôle global du processus.

© IFACI



Bonne Pratique : L'auditeur interne devra :

- *contrôler le bon fonctionnement de cette organisation ;*
- *s'assurer de la mise en œuvre des plans d'actions élaborés par cette organisation ;*
- *vérifier la disponibilité des outils nécessaires à cette mise en œuvre (accès documentaire, web, …).*

3.5.2.2. *Le Plan de Maintien en Condition Opérationnelle (PMCO)*

Le plan de Maintien en Condition Opérationnelle (PMCO) est le guide de mise à jour du PCA.
Ces mises à jour doivent suivre chaque évolution des procédures opérationnelles. L'ensemble des contrôles sera facilité par la mise en place d'un outil de suivi simple et efficace.

Bonne Pratique : il conviendra de disposer d'un plan de mise à jour des procédures opérationnelles tant informatiques qu'organisationnelles pour assurer l'actualisation régulière du PMCO.

L'auditeur interne doit s'assurer que :

- l'organisation du MCO est bien transversale entre processus ;
- les points de vérification de cette transversalité existent bien.

Le PMCO s'élabore dès la phase « Projet », et il est régulièrement mis à jour en fonction des évolutions du PCA. Cette mise à jour s'appuie sur une structure croisée de documents et de faits générateurs (cf. tableau ci-contre).

© IFACI

Exemples de croisement pour la mise à jour du PMCO (documents et faits générateurs)

Document	Mobilité du personnel	Changement de SI	Création nouveau service	Fait générateur
Liste des collaborateurs	Trimestriel		Semestriel	
Liste des fonctions clés	Trimestriel		Semestriel	
Plan de gestion de crise	Trimestriel		Semestriel	Annuel
PSI	Trimestriel	Semestriel	Semestriel	
Plan de repli	Trimestriel		Semestriel	
Document x	Trimestriel			Annuel

Ce tableau peut être complété en spécifiant les documents ou faits générateurs de l'organisation.
Ce PMCO doit également intégrer la mise à niveau des mallettes de crise.
Les mallettes de crise représentent une variété d'éléments indispensables à la bonne reprise de l'activité ; ces éléments sont inclus dans des supports non homogènes et complémentaires. Elles peuvent être différentes et adaptées à leurs utilisateurs.
Les utilisateurs des mallettes de crise sont répertoriés et font l'objet d'un contrôle d'utilisation ; ils sont en mesure d'en justifier l'accessibilité permanente.
Les périodes de mise à jour minimum seront indiquées dans le tableau « faits générateurs » ci-dessus.
Les mallettes de crise sont définies par le Comité de pilotage du PCA et sont toutes conçues sur la base d'un tronc commun.
Elles revêtent des formes variées :

- réseau interne ;
- Web ;
- CD, memory card, clé USB…;
- documentation papier (dossiers, modèles, annuaires, …) ;
- moyens logistiques (paper-board, lampes de poche …) ;
- mallette physique.

Bonne pratique : l'auditeur interne doit s'assurer que :

- *le PMCO est à jour ;*
- *les actions inscrites au PMCO sont bien suivies par le RPCA et ses correspondants ;*
- *les mallettes de crise sont adaptées, complètes, à jour et accessibles ;*
- *des contrôles et des métriques ont été instaurés.*

© IFACI

3.5.2.3. Les tests des solutions mises en œuvre

Les tests et exercices s'adressent à toutes les populations de l'entreprise et s'intéressent à toutes les phases de la gestion de la crise :

- tests techniques (Informatique, téléphonie, réseau, sécurité des SI, …) ;
- tests logistiques (accueil post sinistre, sécurité des personnes et des biens, fonctionnement du site de repli utilisateurs, fonctionnement des salles pour les cellules de crise, …) ;
- exercices opérationnels (sur le(s) site(s) de repli ou non) ;
- mise en situation des cellules de crise (tests RH, d'organisation et de communication).

3.5.2.4. Le RPCA : un rôle fort, un nouveau métier

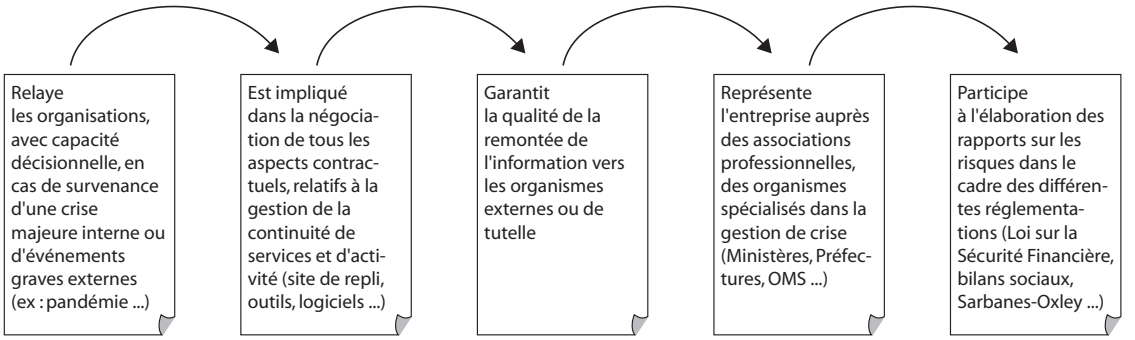
L'audit de la phase MCO est d'abord l'audit de la fonction de Responsable du Plan de Continuité d'activité (RPCA), de la structure mise en place et de ses procédures.
Au quotidien le RPCA dynamise le PCA, il peut être également le responsable de la gestion des incidents et s'assure que le processus MCO est conforme aux directives exprimées par l'entreprise.

Bonne Pratique : Les activités exposées dans le schéma du § 2.2.2. (page 15) donnent des pistes à l'auditeur interne pour construire son référentiel d'audit (classification par thèmes) sur les missions, rôles et fonctionnement du RPCA.

Le RPCA doit intégrer les choix de la politique d'assurance de l'entreprise, en termes de garanties et de couvertures, pour élaborer un PCA adapté et limitant les conséquences financières ou non d'un sinistre grave ou d'une crise.

Le RPCA a un rôle important vis-à-vis des acteurs externes. En effet, le RPCA assure une veille technologique et fonctionnelle. Il a également un rôle de représentation puisqu'il est l'interlocuteur, le point d'entrée de l'entreprise par rapport à l'externe.
Il garantit la conformité du PCA vis-à-vis des instances de tutelle, des régulateurs, du Conseil d'Administration ou de toute instance de surveillance.

Responsabilités du RPCA vis-à-vis des acteurs externes



© IFACI

Le RPCA a également un rôle de vérification qui dépasse les frontières de l'entreprise.

Bonne pratique : Le RPCA doit s'assurer que les contrats de sous-traitance sont conformes, correctement formalisés, respectés, opérationnels et accessibles.

Ainsi, il doit élaborer des tests et exercices avec les partenaires, et peut préconiser un audit en cas de doute. En cas de défaillance du prestataire, le RPCA doit engager le processus d'amélioration auprès des Directions de l'entreprise concernée. Il demande au sous-traitant de se mettre en situation de répondre aux besoins, envisage la révision du contrat, son annulation ou la recherche d'un nouveau partenaire.

Enfin, le RPCA a un rôle important pendant la période de crise. Le RPCA a un rôle d'assistance transverse et de conseil aux cellules de crise et aux coordinateurs :

- procédures d'escalade ;
- procédures de secours ;
- procédures de gestion de crise ;
- procédures de retour à la normale.

Bonne pratique : Lors de la survenance d'une crise totale ou partielle, de par sa connaissance des métiers de l'entreprise et du processus PCA, l'auditeur interne peut être inclus dans le processus de gestion de la crise pour effectuer des missions de surveillance opérationnelle ou de contrôle de l'entreprise.

3.5.2.5. Des moyens à tous les niveaux de l'entreprise

Le RPCA doit être tourné vers les autres acteurs de la gestion de crise, en particulier les CCA et la Direction Générale.
Le RPCA :

- informe les CCA sur les évolutions ;
- s'assure que les CCA intègre le thème du PCA dans leur processus de maîtrise des risques ;
- veille à la prise en compte des besoins des CCA dans le cahier des charges des tests et exercices du PCA ;
- les associe à la réalisation des tests et exercices ;
- diffuse aux CCA les analyses des impacts de toute évolution fonctionnelle, logistique, informatique et humaine, sur la continuité d'activité en anticipation sur le plan ;
- leur apporte les outils spécifiques et les formations nécessaires.

Le RPCA diffuse auprès de la Direction Générale un ensemble de reportings tels que :

- le tableau de bord de la continuité d'activité (Cf. fiche technique n°9, p.79) ;
- des bilans synthétiques des exercices ;
- des rapports annuels d'activité.

© IFACI

3.5.2.6. Zoom sur les tests et exercices

La planification des tests et exercices est réalisée lors de la phase « Projet » puis, lors de la phase « MCO », par le Comité de Pilotage du PCA (sous l'égide du RPCA et du RSSI pour en assurer l'opérationnalité et la sécurité).
Les tests peuvent être complets ou bien modulaires. Ils seront considérés comme significatifs dès lors qu'ils auront porté avec un succès suffisant sur un ensemble cohérent (scenario, plan, site …). C'est le RPCA qui valide un passage en MCO suite à ces tests et exercices.
L'auditeur interne peut avoir un double rôle dans ce cadre :

- vérifier les plans et procédures de tests :
  - ils sont réalisés selon la méthode des scénarios (immobilier, informatique, RH) ou correspondent à des processus ;
  - ils doivent impliquer l'ensemble des acteurs utiles à leur réussite ;
  - ils couvrent progressivement l'ensemble des activités essentielles de l'entreprise ;
  - ils intègrent les métiers opérationnels, les fonctions techniques et support, les cellules de crise ;
- assurer l'audit sur place des tests et exercices (cf. fiche technique n°3, p.60).

3.5.2.7. Zoom sur les structures complexes (groupe, filiales)

La filiale doit s'assurer de la conformité de son PCA avec les règles et les méthodes imposées par le Groupe.
La filiale s'appuie sur les travaux du RPCA du Groupe et dispose d'une capacité décisionnelle et budgétaire propre lui permettant de gérer de manière autonome toute crise.
Il est également conseillé :

- de tendre vers une mutualisation des moyens (même dans le cadre d'un éloignement géographique) ;
- d'être vigilant sur l'application des consignes du Groupe, leur intégration dans les consignes de filiale et l'adéquation des budgets dédiés ;
- d'examiner la cohérence de la mutualisation éventuelle des moyens ;
- et de s'assurer que les solutions retenues sont bien opérationnelles et correctement formalisées.

3.5.3 Les objectifs d'audit et les principaux risques associés

Les thèmes de la phase « MCO » à examiner pour l'audit interne ont été présentés dans le paragraphe précédent.
Ces sujets d'audit sont précisés dans le tableau ci-après par des objectifs d'audit ainsi que les risques associés.

© IFACI

Objectifs d'audit	Risques
Préparation de l'environnement nécessaire au MCO	Défaut ou manque de positionnement Inadéquation des moyens et ressources
Formalisation du passage en MCO Organisation générale du fonctionnement Documentation générale sur la phase (stockage, accès et contrôles d'accès, liens documentaires, mises à jour, liste de diffusion)	Défaut de formalisation du PCA Absence, inadéquation ou non respect de la procédure, de la méthode ou de la norme
Prise en compte des différents scénarios	Périmètre insuffisant ou inadéquat
Révision périodique de l'analyse des risques et des bilans d'impacts sur activités	Utilisation de documents obsolètes Utilisation de données erronées
Modalités retenues pour la communication interne	Communication de crise absente ou insuffisante Communication d'informations ou de données inexactes ou insuffisantes Destinataires inappropriés
Animation des correspondants	Insuffisance de la structure de pilotage Maillage inefficace Procédures PCA non mises à jour
Représentation de l'entreprise vers l'externe Communication externe	Risque d'image
Contrôle du processus de continuité d'activité (tous niveaux de contrôles)	Insuffisance du système de contrôle interne (contrôles permanent et périodique)
Intégration de la continuité d'activité dans la gestion de crise	Défaillance de retour d'expérience et dans la boucle d'amélioration du PCA
Formations et informations en interne	Besoin de formation non identifié Défaut de formation
Coordination avec le PCA des sous-traitants	Dépendance à l'égard de la défaillance d'un prestataire
Suivi budgétaire	Anticipation insuffisante ou inadéquate des charges et des moyens Ressources matérielles insuffisantes ou inadaptées
Suivi des tests et exercices (calendrier, nature, périmètre, historique)	Absence ou insuffisance de back-up Absence ou insuffisance de sécurisation du système d'information Destruction ou dégradation des biens de l'entité Destruction ou dégradation des biens des clients
Outils de gestion du PCA (mallette, site Web, logiciels, mémos …)	Moyens inadaptés, insuffisants ou inexistants

© IFACI

Bonne Pratique : Compte tenu de ces nombreux objectifs d'audit, une inscription régulière, voire fréquente, du PCA (dans sa globalité ou selon des domaines spécifiques) au plan d'audit assurera une bonne mesure de l'efficience du processus et de la maîtrise des risques résiduels.

3.5.4. Les conseils pour accompagner l'audit de la phase MCO

Le nouveau métier de Responsable du Plan de Continuité d'Activité (RPCA) et la mise en œuvre d'un processus inédit (pas toujours achevé) nécessitent une vigilance particulière de l'audit interne qui doit s'adapter à une vision différente de l'entreprise, parfois déstabilisante.

Les plans d'audit sur le sujet seront donc particulièrement préparés et intégreront des notions allant au-delà de la réglementation selon la règle de "la bonne logique terrienne".

En général, les plans d'audit de la continuité d'activité varieront pendant les premières années (projet, mise en œuvre des solutions, "rodage" de la fonction et des processus) de la vie du PCA. Ensuite, le plan est stabilisé, car la continuité d'activité rentre dans les mœurs de l'entreprise, et les solutions majeures deviennent opérantes.

La réussite du maintien en condition opérationnelle dépend de la volonté de l'entreprise de pérenniser l'organisation de crise, de finaliser le Plan MCO et de l'appliquer dans le temps ; sur ces trois thèmes, l'audit interne peut jouer un rôle essentiel.

Le renfort d'une ressource externe spécialisée est une opportunité à étudier sérieusement, non seulement en raison du niveau de qualification immédiatement opérationnelle, mais également pour assurer un transfert de connaissances.

Bonne pratique : on trouvera le guide d'audit de la phase « Maintien en condition opérationnelle » dans la fiche technique n°4, p.63.

© IFACI

CONCLUSION

Dans un contexte où, toutes entreprises confondues, l'audit interne se trouve de plus en plus souvent sollicité pour vérifier la conformité aux obligations réglementaires, l'audit du Plan de Continuité d'Activité apparaît particulièrement instructif et valorisant. Qu'il s'agisse de la méthode retenue pour la mise œuvre du Plan de Continuité d'Activité, des modalités de gestion, des environnements et des résultats des tests, plusieurs sujets, allant au-delà des questions de conformité, peuvent être inscrits au plan d'audit interne.

Un des fondamentaux de la continuité d'activité implique que le plan est constitué pour aboutir, en fonction de priorités définies, à un retour progressif des activités vers une situation normale, au moyen de procédures spécifiques, spécialement étudiées pour ces situations. Tout est dit ! Voici la ligne de mire du Responsable du Plan de Continuité d'Activité et les thèmes d'audit à partir desquels l'auditeur interne déclinera son référentiel.

La nécessité de la continuité des activités en cas de choc extrême n'est pas un processus marginal ou exogène ; il doit s'intégrer à la culture d'entreprise et à la réflexion stratégique à tous les niveaux de responsabilité et dans tous les développements des activités. C'est la gouvernance de l'entreprise qui est en première ligne et dans cette prise de conscience l'audit interne dont les missions contribuent à la gouvernance.

En matière de Plan de Continuité d'Activité, il n'y a pas de phase plus importante que celle dans laquelle on se trouve. Il est important de ne pas anticiper, il est sage de ne pas vouloir afficher l'atteinte de la phase « Maintien en Condition Opérationnelle » sans avoir "bouclé" les préalables. Le respect de ces préalables est un objectif d'audit primordial.

Le Responsable du Plan de Continuité d'Activité exerce souvent un nouveau métier qui nécessite la mise en œuvre de nouveaux processus, voire la prise en compte de nouveaux risques. L'audit interne doit intégrer ces nouveaux thèmes d'audit, adapter fréquemment ses référentiels, surtout les plus techniques (tests et exercices). Le Plan de Continuité d'Activité est réactualisé en permanence pour de nombreuses raisons : cession ou acquisition, créations de nouveaux sites ou produits, modification sur les Ressources Humaines, cession ou acquisition d'un site de repli... Toutes ces situations justifient des audits fréquents sur la gestion du plan et sur les tests.

Le responsable de l'audit interne doit s'assurer que chaque mission d'audit, quel que soit le processus audité, comporte un thème « Plan de Continuité d'Activité » pour permettre de se poser des questions telles que :

- la criticité du processus a-t-elle été évaluée ? Comment ?
- depuis cette évaluation, les paramètres ont-ils changé ?
- les procédures de continuité d'activité couvrent-t-elles l'ensemble du processus ?
- si le processus est pris en charge dans le Plan de Continuité d'Activité, a-t-il été testé ?
- comment l'externalisation complète ou partielle du processus est-elle prise en compte ?
- la Durée Maximum d'Interruption de l'Activité a-t-elle été minorée ? Est-elle acceptable ?

Face à la complexité du sujet à couvrir, il convient de veiller à l'anticipation des formations pour obtenir les compétences nécessaires au sein de l'équipe d'auditeurs internes.

L'audit interne peut contribuer à la promotion des processus de continuité d'activité. En effet, la pérennité de l'entreprise est un but tout à fait cohérent avec les objectifs essentiels de l'audit interne, gardien du système de contrôle interne et de la sécurité des actifs. A ce titre, il pourra autant que de besoin favoriser l'émergence d'une charte de gestion et de

© IFACI

contrôle de la continuité d'activité. Concomitamment à des missions sur le Plan de Continuité d'Activité, l'audit interne contribue à l'amélioration du contrôle interne de l'entreprise et enrichit son référentiel d'audit.
A l'issue d'une réflexion approfondie sur la mise en place de procédures dégradées en cas de crise, la continuité d'activité entraîne l'attribution de budgets importants qui rend d'autant plus nécessaire la recherche de "Return on Investment" (ROI).
L'audit interne contribue à cette réflexion en développant des constats et des recommandations relatifs :

- au renforcement de la gouvernance (Cellule de Crise Décisionnelle / Opérationnelle),
- à la qualité des procédures de gestion,
- à l'amélioration de la sécurité immobilière (surveillance et maintenance technique),
- à une meilleure surveillance de l'activité des prestataires extérieurs,
- à une meilleure connaissance des couvertures de risques (adéquation des assurances,…)…

Enfin, l'efficacité des solutions de continuité d'activité implique une diminution des délais maximaux d'interruption admissibles et renforce globalement la sécurité et l'image de l'entreprise.
La perspective malheureusement envisageable de survenance d'une crise et la prise en compte managériale de cette situation potentielle donnent à l'entreprise l'opportunité d'améliorer son système de contrôle interne et à l'audit interne la chance d'y contribuer.

© IFACI

SIGLES ET GLOSSAIRE

Sigles :

BIA ..... Bilan d'Impact sur Activités
CCA ..... Correspondant Continuité d'Activité
CCD ..... Cellule de Crise Décisionnelle
DMIA ..... Délai Maximal d'Interruption Admissible
MCO ..... Maintien en Condition Opérationnelle
PCA ..... Plan de Continuité d'Activité
PCIT ..... Plan de Continuité Informatique et Télécommunications
PCO ..... Plan de Continuité des Opérations
PMCO ..... Plan de Maintien en Condition Opérationnelle
PMDA ..... Perte Maximale de Données Admissible
PSI ..... Plan de Secours Informatique
RPCA ..... Responsable du Plan de Continuité d'Activité
RSSI ..... Responsable de la Sécurité des Systèmes d'Information

Glossaire :

Bilan d'impact sur activités

Processus qui consiste à identifier et mesurer (quantitativement et qualitativement) l'impact sur l'activité ou les pertes dans les processus métiers en cas de perturbation. Il est utilisé pour identifier les priorités de reprise, les besoins en ressources pour la reprise, le personnel essentiel et pour aider à formuler un plan de continuité d'activité.

Continuité d'activité

Ce terme désigne la permanence et le maintien des opérations considérées comme majeures par l'entreprise selon des modes opératoires adaptés à la survenance d'événements d'une gravité exceptionnelle.

Délai de reprise

Durée cible nécessaire à la reprise d'une opération professionnelle spécifique. Le délai de reprise a deux composantes : la durée de l'interruption jusqu'à l'activation d'un plan de continuité d'activité et la durée depuis l'activation du plan de continuité d'activité jusqu'à la reprise de l'opération professionnelle spécifique.

© IFACI

Délai Maximal d'Interruption Admissible

Le délai maximal d'interruption admissible après un sinistre correspond à la période de temps au bout de laquelle les fonctions de service doivent impérativement être restaurées. Le DMIA des fonctions ou services métiers doit être défini dans le PCA.
Le DMIA des services et applications informatiques doit être cohérent avec le DMIA des métiers. Le terme anglo-saxon correspondant est RTO : recovery time objective.

Gestion de la continuité d'activité

Une approche globale qui comprend la politique, les règles et les procédures, garantit en cas de perturbation le maintien ou la reprise planifiée des opérations spécifiques. Son but est de réduire au minimum les conséquences opérationnelles, financières, légales, de réputation et autres conséquences substantielles d'une perturbation.

Opération ou service critique

Activité, fonction, processus ou service, dont la perte aurait des conséquences substantielles pour la continuité des opérations du système financier concerné. La détermination du caractère "critique" d'une opération ou d'un service particulier dépend de l'entreprise. Les opérations de centre de calcul sont un exemple d'opérations critiques pour la plupart des acteurs.

Perte maximale de données admissible

Le temps de latence entre un état stable de restauration et le sinistre. Par exemple, si les sauvegardes de fichier sont réalisées chaque nuit, un sinistre dans la journée correspondra à une PMDA de 24 heures, puisque les données de la journée d'exploitation où a eu lieu le sinistre seront perdues et qu'on ne pourra restaurer qu'à partir de l'état stable de la veille. Le terme anglo-saxon correspondant est RPO : recovery point objective.

Plan de continuité d'activité

Le plan de continuité d'activité est un composant de la gestion de la continuité d'activité. Un plan de continuité d'activité est un plan d'action écrit, complet, qui expose les procédures et les systèmes nécessaires pour poursuivre et rétablir les opérations d'une organisation en cas de perturbation.

Plan de Continuité Informatique et Télécommunications

Le plan de continuité informatique et télécommunications est un ensemble de procédures et de dispositions prévues pour garantir à l'entreprise la reprise de son système informatique et télécommunications en cas de sinistre.

Plan de Maintien en Condition Opérationnelle (PMCO)

Le plan de maintien en condition opérationnel est le guide de mise à jour du PCA.

© IFACI

Plan de Secours Informatique

Un plan de secours informatique est conçu pour gérer le risque de perte des ressources informatiques, essentiellement matérielles et logicielles.
En ceci il ne doit pas être confondu avec le PCA (Plan de Continuité d'Activités) de la fonction informatique, qui gère le risque de perte de ressources le plus souvent logistiques, humaines, de locaux, de transports...
Le PSI est donc complémentaire de l'ensemble des PCA des fonctions et services de l'entreprise et, réunis, ils forment le Plan de Continuité d'Entreprise.

Reprise

La reconstruction d'opérations spécifiques après une défaillance, à un niveau suffisant pour satisfaire les obligations professionnelles essentielles.

Résilience

La capacité d'un acteur, quel que soit son secteur économique, à absorber l'impact d'une perturbation opérationnelle majeure et poursuivre les opérations ou les services critiques.

Site alternatif

Un site tenu prêt pour utilisation lors de la survenance d'un événement menaçant la continuité d'activité. Le terme s'applique également aux besoins d'espaces de travail et de technologies. Dans quelques cas, un site alternatif peut contenir les équipements qui sont utilisés pour des opérations quotidiennes normales, mais qui sont capables d'accueillir des activités supplémentaires.

© IFACI

© IFACI

FICHES TECHNIQUES

1 - Recueil des informations nécessaires lors de la phase d'audit « Etat des lieux »

2 - Guide d'audit de la phase « Projet » du PCA

3 - Guide d'audit de la phase « Tests et Validation » du PCA

4 - Guide d'audit de la phase « Maintien en condition opérationnelle »

5 - Guide d'audit du Plan de Secours Informatique (PSI)

6 - Assurance et audit de PCA

7 - Référentiel de bonnes pratiques : communication interne, formation et PCA

8 - Charte du PCA

9 - « Feuille de route » du RPCA

10 - Bilan d'impact sur activités du PCA

11 - Questionnaire d'auto – évaluation de PCA

© IFACI

1- Recueil des informations nécessaires lors de la phase d'audit « Etat des lieux »

Dix domaines d'investigation sont proposés pour évaluer le processus de décision relatif à l'opportunité de lancer ou non un PCA.
Le tableau suivant classe les items dans l'ordre de traitement préconisé pour réaliser une mission d'audit de conseil, sur un périmètre donné.

Paramètres	Sources des informations	Evaluer les paramètres[1] *1 : faible* *2 : modéré* *3 : fort*	Analyser les paramètres ou Comment faire un état des lieux ?	Retenir des axes d'investigation
1. RESULTAT PAR ACTIVITE	1. Tableaux de bord du contrôle de gestion interne. 2. Résultat mensuel par activité. 3. Résultat comptable du mois.		Mesurer la contribution au résultat de l'entreprise et au résultat de la maison mère.	A-t-on évalué leur contribution aux résultats de l'entreprise ?
2. LIGNES D'ACTIVITES PRIORITAIRES	1. PV des organes exécutifs et délibérants. 2. Critères de priorisation (politiques, financiers…) 3. Plan de développement		Identifier les développements d'activité ayant fait l'objet d'examens et de décisions par les organes exécutifs et délibérants. Préciser les priorités Groupe/local.	- A-t-on identifié les activités critiques ?
3. ELEMENTS CLES DE LA LIGNE D'ACTIVITE : - PROCESSUS « CŒUR D'ACTIVITE » CRITIQUES, PROCESSUS SUPPORT CRITIQUES	1. Politique adaptée par les organes de gouvernance. 2. Instructions de l'organe exécutif 3. Plan financier annuel 4. Données économiques et techniques (chiffre d'affaires, coût, délais, communication) 5. Business Plan sur les activités nouvelles		Examiner la stratification de la clientèle (institutionnels, particuliers, grossistes, détail). Etudier le plan commercial annuel et pluriannuel (responsables et objectifs à atteindre).	- Quelles sont les parties prenantes prioritaires ? - A-t-on identifié, évalué, fixé, les délais d'indisponibilité acceptables des activités ? À classer par parties prenantes, notamment vis à vis des clients externes et internes ?

[1] *Selon la modélisation et le référentiel propre à l'entreprise, il s'agira de l'impact financier, de la criticité, de la « value at risk » (VAR).*

© IFACI

Paramètres	Sources des informations	Evaluer les paramètres[1] *1 : faible* *2 : modéré* *3 : fort*	Analyser les paramètres ou Comment faire un état des lieux ?	Retenir des axes d'investigation
4. ANALYSE RISQUES	1. Cartographies risques : gestion risques, audit interne, commercial, marketing . 2. Scénarios de menaces étudiés		Evaluer les risques Exploiter la base d'incidents avérés. Identifier tous les contrôles destinés à réduire les risques. Identifier les limites de risques tolérés.	- Quels sont les risques à couvrir ? identification, évaluation des impacts, niveaux d'acceptabilité (décisions), plans de traitement ou de couverture ?
5. SYSTEMES D'INFORMATION	1. Direction des systèmes d'information. 2. Procédures opérationnelles 3. Documentation du contrôle interne effectué. 4. Rapports de communication interne et externe sur les lignes d'activités prioritaires et sur les remontées filiales-Maison mère		Identifier tous les flux d'information et les procédures concourant à l'activité. 12. Identifier tous les rapports internes et externes sans lesquels une décision ou une action ne peut être validée.	- A-t-on identifié et pondéré les flux d'information liés aux activités critiques ?

[1] *Lorsque seront interviewés les services en charge de lignes d'activité prioritaires et/ou de fonctions support critiques, on examinera la démarche utilisée pour déterminer le risque résiduel post mise en œuvre d'un PCA.*

© IFACI

Paramètres	Sources des informations	Evaluer les paramètres *1 : faible* *2 : modéré* *3 : fort*	Analyser les paramètres ou Comment faire un état des lieux ?	Retenir des axes d'investigation
6. RESSOURCES	**Ressources internes :** 1. Direction générale 2. Ressources humaines 3. DSI 4. Direction financière 5. Direction commerciale 6. Opérations dédiées 7. Autres fonctions support transversales **Ressources externes :** 1. Externalisation activités. Prestataires sous-traitants		Identifier les moyens nécessaires à un fonctionnement normal. Evaluer les moyens minima pour atteindre l'objectif de continuité par ligne d'activité ou par contributeur.	- Quels sont les acteurs internes de l'entreprise à coordonner ? - A-t-on une cartographie des ressources de l'entreprise (internes et externes) ?
7. PROCEDURES METIERS	1. Procédures rédigées (standards, en mode d'activité normale) 2. Le cas échéant une étude de chaîne de valeur, de remise à plat des processus (re-engineering des processus)		Documenter les procédures des processus significatifs répondant à une continuité d'activité.	- Quels liens existe-t-il avec les procédures en mode dégradé ? - A-t-on identifié, évalué, décidé, les délais d'indisponibilité acceptables des activités ? À classer par parties prenantes, notamment vis à vis des clients externes et internes ? - A-t-on à disposition une cartographie des procédures d'activités en mode normal ?

© IFACI

Paramètres	Sources des informations	Evaluer les paramètres *1 : faible* *2 : modéré* *3 : fort*	Analyser les paramètres ou Comment faire un état des lieux ?	Retenir des axes d'investigation
8. ACTEURS POTENTIELS DU DOSSIER PCA	1. Système de délégations de pouvoirs de l'entreprise			Existe-t-il des lettres de mission relatives à l'étude du dossier PCA, notamment dans les domaines juridique, communication, finance, ressources humaines, logistique, informatique, sécurité ?
9. REGLEMENTATION	1. Service juridique 2. Politique de Conformité 3. Contrats		Identifier tous les incidents liés au service juridique (litiges, réclamations, amendes, pénalités) ayant un lien avec la continuité des activités de l'entreprise. Identifier les réglementations locales (maison mère, pays d'implantation des filiales sur les points essentiels en matière de couverture du risque de non continuité).	- Y-a-t-il des évolutions réglementaires qui pourraient impacter le dossier PCA ?

© IFACI

Paramètres	Sources des informations	Evaluer les paramètres *1 : faible* *2 : modéré* *3 : fort*	Analyser les paramètres ou Comment faire un état des lieux ?	Retenir des axes d'investigation
10. ELEMENTS DE L'ECONOMIE GLOBALE DE LA DEMARCHE PCA	1. chiffrage global de la phase réflexion à la phase MCO. 2. impacts du projet en termes de mobilisation des ressources et d'indisponibilité des activités opérationnelles et/ou des revenus correspondants.		Benchmark (entreprises comparables) Identification des synergies par pays et/ou par activité pour « bâtir » cette réflexion	- L'étude du coût d'un PCA fait partie de l'audit des phases « Projet » et « MCO »

Cette analyse vient alimenter les objectifs clés de la mission d'audit relative à la phase « État des lieux ».

© IFACI

2- Guide d'audit de la phase « Projet » du PCA

La phase « Projet » du Plan de Continuité d'Activité s'articule autour de 6 étapes clés. La mission d'audit peut s'appuyer sur le tableau suivant pour mener ses analyses.

Les vérifications à mener portent sur l'existence et le contenu des étapes :

Thèmes	Bonnes pratiques
Revue du dispositif global (élaboration et organisation des plans généraux transverses à l'entreprise tels que RH, communication,…)	• Des interviews permettent de vérifier l'adaptation et l'efficience du dispositif organisationnel ; • S'assurer qu'il existe un processus de renouvellement des membres du dispositif (turn-over, changement d'organisation) ; • Constater la communication régulière et la prise en compte des changements intervenus.
	• Effectuer un rapprochement avec les référentiels constitués lors d'autres missions d'audit ou lors de la phase « État des lieux » ; • S'assurer de la cohérence entre le référentiel d'activités utilisé dans le projet PCA et l'organigramme mis à jour.
	• Constater la validation, la clarté, la diffusion du projet de procédure générale du PCA, rédigé par le RPCA ; • Vérifier que les modalités de déclenchement du PCA sont précisées.
	• S'assurer que les risques opérationnels considérés comme significatifs lors de la phase « État des lieux » sont tous couverts par un PCA. Inversement, identifier les risques non significatifs couverts par le PCA (ce niveau de couverture est-il efficient ?).
	• Vérifier que l'expression de besoins de continuité peut être actualisée si nécessaire ; • S'assurer que le projet PCA a prévu les conditions d'intégration de toute nouvelle activité critique ou projet informatique ; • Vérifier que tous les composants existants du PCA pourront être actualisés et testés régulièrement ; • A chaque phase réalisée, vérifier que la communication aux acteurs, au personnel et aux organes représentatifs du personnel (CHSCT, Comité d'entreprise) est faite et que des formations régulières sont assurées.
	• Le reporting budgétaire permet-il une correcte affectation de la dépense, le déroulement du calendrier et la mise en évidence des retards ou des dépassements ? • Le reporting budgétaire se distingue-t-il du budget informatique, hors PSSI ? • Le reporting budgétaire concerne-t-il l'ensemble des coûts budgétés, y compris les coûts internes ? • Le reporting budgétaire fait-il l'objet d'une validation régulière par les instances de pilotage ?

© IFACI

Thèmes	Bonnes pratiques
Revue du dispositif global (élaboration et organisation des plans généraux transverses à l'entreprise tels que RH, communication,…) (suite)	• Se reporter à la fiche technique « Questionnaire d'auto-évaluation », p.86.
	• Envisager l'audit du PCA, de ses activités sous-traitées dans la mesure où le contrat le permet ; • S'assurer que des clauses d'auditabilité sont prévues dans les contrats.
	• S'assurer de la conformité du processus du chômage technique, du travail à domicile, des congés forcés, de délocalisation du lieu de travail, du recours à des prestataires de services…
	• Vérifier qu'un tel dispositif existe et permet de donner des consignes claires pour assurer de façon optimale le déclenchement du plan de secours.
	• Est-il mis en œuvre auprès de tous les acteurs (métiers et support) concernés ?
	• Vérifier que la répartition des rôles est claire et permet une information externe efficiente, en particulier vis-à-vis des médias.
Audits des plans de secours organisationnels par activité	• Ces procédures doivent être validées, claires, diffusées et à jour. Les procédures permettent : - l'identification des opérations maintenues ou suspendues, - l'ordonnancement des opérations maintenues, - l'identification des collaborateurs et fournisseurs mobilisables.
Audits des plans de secours techniques	• Vérifier le cahier des charges pour développer le back-up informatique retenu/choix de maître d'œuvre/prestataire ; vérifier la qualité des équipes prévues pour administrer le dispositif retenu (nombre, profils,…) ; • Vérifier la conformité de la démarche de recherche des intervenants ou prestataires extérieurs (hébergeurs, sites de repli) avec le cadre arrêté lors de l'état des lieux ; • Evaluer la cohérence de chaque contrat signé avec le budget, le calendrier, les impératifs de sécurité ; • Vérifier la présence d'une clause PCA dans les contrats de prestations, si un contrôle préalable sur ce thème a été réalisé chez le prestataire. Le cas échéant, obtenir les résultats d'un contrôle préalable du PCA du prestataire ; • Vérifier l'existence d'un procès-verbal de recette.
	• Hormis pour les entreprises qui se créent, le Plan de Secours Informatique (PSI) (qui comprend le back up des ressources informatiques) est dans la majorité des cas, préexistant. Il convient donc de vérifier que les plans de secours techniques sont parfaitement réajustés avec le projet global PCA. • Détecter les éventuelles absences de PCA pour des services critiques.

© IFACI

Thèmes	Bonnes pratiques
Efficience de la cellule de crise	• S'assurer de l'existence de tests de situation de crise, prévoir d'auditer les exercices avant la recette du PCA. • Eviter d'évaluer "à chaud" la pertinence des décisions prises, démarche qui demande des investigations plus approfondies ; • L'auditeur interne devra apprécier les points suivants : - la pertinence du rythme des tests, - l'efficience du RPCA, sa capacité à mobiliser et à se faire entendre, à rectifier les comportements non conformes, à alerter au plus haut niveau en cas de blocage, - la disponibilité et l'actualisation des outils (annuaires, fournisseurs, relais de la place, contrats en cours…), - la disponibilité des procédures et la qualité de leur mise à jour, l'efficacité de la cellule, la capacité à avoir un reporting de l'état de la crise, à prendre des décisions, - le traitement des anomalies détectées à l'issue des tests. • Implication de l'auditeur interne à chaque test en tant qu'observateur si participant à la cellule de crise : - support d'audit à prévoir, rapport d'audit à réaliser, recommandations, retour des plans d'action demandés et exposés en Comité de pilotage.
Audit des reportings périodiques faits au Comité d'audit, aux Comités de pilotage et à toute instance décisionnelle	• Vérifier la qualité du plan d'action qui doit toujours reprendre l'historique, le réalisme du planning en regard des ressources ; • Vérifier l'intégration des nouvelles missions dans le périmètre PCA.
Audit de la gestion des incidents	• Recenser la nature des incidents, leur mode de prise en compte et de résolution (procédure d'alerte, procédure d'escalade,…) ; • Identifier des zones insuffisamment couvertes ou non couvertes par le PCA, qui doivent faire l'objet de recommandations ; • L'auditeur interne veillera à limiter l'exploration de la gestion des incidents qui peut constituer à lui seul une mission d'audit complète.

© IFACI

3- Guide d'audit de la phase « Tests et Validation » du PCA

1 - Aspects à aborder lors du test initial d'un PCA :

Il s'agit principalement de s'assurer que :

- le PCA est en ligne avec la stratégie de l'entreprise ;
- le management s'est formellement engagé dans l'élaboration du PCA ;
- la mise en œuvre a respecté les jalons clés du mode projet.

Objectif de contrôle	Activité de contrôle	Axes d'investigation	Exemples de questions dans le domaine des SI
La stratégie de tests est définie et est en ligne avec les scénarios de sinistres retenus	Les exigences de test du PCA sont formellement définies dans des Politiques, Standards et Procédures de l'entreprise.	- Analyser les Politiques, standards et procédures définis par l'entreprise dans le domaine du PCA. - Identifier les scénarios de sinistre couvert par le PCA. - Identifier les exigences légales et réglementaires auquel le secteur d'activité de l'entreprise est soumis. - Apprécier les ressources et moyens attribués à la phase de tests du PCA. - Les responsabilités relatives aux tests du PCA ont-elles été clairement attribuées ?	Est-ce que chaque évolution est suivie de tests ?

© IFACI

Objectif de contrôle	Activité de contrôle	Axes d'investigation	Exemples de questions dans le domaine des SI
Les tests sont réalisés conformément au plan de tests	Les tests doivent être effectués régulièrement	- Examiner les comptes rendus des tests et exercices des deux dernières années. - Analyser la planification des prochains tests.	Y a-t-il au moins une série de tests par an sur les dispositifs les plus critiques ? Selon quelle(s) fréquence(s) la solution de secours est-elle testée ?
	Les tests doivent couvrir tout le périmètre du PCA	- Tester le PCA chez un prestataire externe.	La solution de secours est-elle complètement testée ?
	Le plan de tests définit l'organisation, la modalité, la nature et l'ordonnancement des tests.	Les employés ont-ils été informés de l'existence des plans de tests et procédures ? Le contenu du plan de tests est-il adéquat et précis ?	Le plan de tests comporte-t-il des tests techniques unitaires, tests étendus et/ou complémentaires, tests en situation réelle ? Réalise-t-on périodiquement ou de manière impromptue un inventaire et une relecture (par exemple sur lots ou échantillons cycliques) des sauvegardes des fichiers stratégiques en fonction de la périodicité de mise à jour, de la classification des contenus et de la qualité du support ? Selon quelle(s) fréquence(s) ?
Le résultat des tests doit être documenté et transmis au management et validé	Le rapport des tests est rédigé et diffusé	- Le rapport est-il probant ? - Vérifier la transmission du rapport au niveau de décision approprié.	Y a-t-il eu une recette avalisée par le prestataire de service et l'utilisateur fondée sur un essai réel concluant ? Chaque test fait-il l'objet d'un compte rendu ? Le rapport des tests a-t-il été transmis aux instances de direction et/ou de contrôle ad'hoc ?

© IFACI

Objectif de contrôle	Activité de contrôle	Axes d'investigation	Exemples de questions dans le domaine des SI
Un plan d'action doit être réalisé et mis en œuvre	Analyse des résultats et proposition d'actions de correction et d'amélioration	- Constater que le plan d'action est complet (objectif, actions, délais, responsabilité). - Vérifier la mise en œuvre du plan d'action.	

© IFACI

4- Guide d'audit de la phase « Maintien en Condition Opérationnelle »

L'auditeur interne :

- vérifiera l'adéquation du PCA avec les règles émises par l'entreprise (Plan de MCO) et les meilleures pratiques ;
- recherchera les preuves de la performance des solutions retenues, de leur adéquation aux besoins, de la fréquence des mises à jour et de l'intégration du sujet de la continuité d'activité dans la culture d'entreprise ;
- doit être formé au PCA et aux tests/exercices afin d'assurer son engagement en toute connaissance de cause ;
- pourra contrôler la limitation des risques liés à la gestion de crise, depuis la phase d'alerte jusqu'à la phase du retour à la normale ;
- vérifiera la mise en œuvre des décisions prises à l'issue de la phase de retour d'expérience.

a) Les thèmes à auditer :

Est proposée une répartition issue d'expériences réussies et qui a le mérite de passer en revue l'ensemble des thèmes à auditer dans le cadre d'un audit global du PCA d'une entreprise.

PILOTAGE	1. Stratégie
	2. Communication / Sensibilisation
	3. Organisation générale
	4. Couverture du PCA
ORGANISATION DÉTAILLÉE	5. Plan de gestion de crise
	6. Plan de repli
	7. Plan de communication de crise
	8. Ressources humaines
	9. Système d'information et télécom
	10. Logistique et sécurité
	11. Métiers / Filières & Services
DOCUMENTATION	12. Archivage / Documentation
TESTS ET EXERCICES	13. Tests
	14. Exercices
MAINTIEN EN CONDITION OPÉRATIONNELLE	15. Maintien en condition opérationnelle

© IFACI

b) Le processus d'audit

La fonction de surveillance permanente est assurée par le RPCA et ses relais. L'audit interne doit intégrer l'évaluation périodique du PCA et du PMCO dans le plan pluriannuel (fréquence rapprochée dans les premières années après la phase projet). Les missions sont priorisées éventuellement à la demande du RPCA.

Le cadrage de la mission doit tenir compte des thèmes et processus suivants :

- existence d'une **auto-évaluation** intégrée dans les pratiques de contrôle interne des entités fonctionnelles et opérationnelles,
- prise en compte systématique de la continuité d'activité lors d'un audit de filiale, d'entité ou thématique,
- conformité et efficience de l'organisation retenue, des processus et des solutions mises en place,
- procédures, documentations fonctionnelles et techniques, cartographies en fonction des niveaux d'intervention (présence, accessibilité, fréquence des mises à jour, homogénéité, degré d'appropriation …),
- existence d'une démarche commune avec la Qualité,
- plans de tests annuels et pluriannuels, tests unitaires et globaux avec repli au moins partiel (informatique, logistique, transversaux, cellules de crise, sites de repli, partenaires …),
- rapprochement des cartographies avec la Direction des risques et la DSI,
- mise en cohérence des référentiels (recueil de l'existant et des besoins, référentiel du RSSI, référentiel RH, référentiel réglementaire …)
- conformité de la sous-traitance (clauses des contrats) :
- intégration de la notion de PCA dans les contrats de prestations de services essentielles,
- vérification de l'adéquation des prestations obtenues (vérifier la permanence),
- continuité de l'action de l'audit interne vers le sous-traitant (possibilité d'auditer chez le prestataire, participation à des missions et des tests en commun, communication des rapports de mission du prestataire),
- existence d'une charte de fonctionnement en phase « MCO ».

© IFACI

5- Guide d'audit du Plan de Secours Informatique (PSI)

Le PSI peut être audité suivant plusieurs approches, soit :

- en tant qu'élément d'une mission plus importante ;
- en termes de revue de projet (en développement ou en bilan) ;
- dans le cadre d'une programmation pluriannuelle d'audit du ou des PSI.

1. *Points clés à vérifier*

• *Quelques points de contrôle essentiels pour l'auditeur interne*

Dans le cas où le PSI est l'un des volets d'une mission, l'audit interne disposera de peu de ressources et devra se concentrer sur des points essentiels, comme par exemple :

- la gestion des sauvegardes, des données, des traitements, et notamment la sécurité de leur stockage et le test de leur intégrité ;
- l'existence d'une politique de sécurité des technologies de l'information. Cette politique devra, entre autres, prévoir la qualification des informations par leur propriétaire en termes de disponibilité, confidentialité, intégrité, auditabilité. Cette politique est basée sur une évaluation des risques ;
- la cohérence de la qualification des informations, en termes de disponibilité avec les DMIA (délai maximal d'interruption admissible) de fonctions et métiers correspondants, définis lors des PCA ;
- le choix des solutions de secours cohérent avec la sensibilité des informations secourues ;
- les engagements des fournisseurs concernant les dispositifs et services de secours ;
- la qualité de la préparation et du test de la gestion des crises.

On pourra consulter l'article "understanding data classification based on business and security requirements" de Rafael Etges et Karen McNeil sur le Journal Online du site de l'ISACA (http://www.isaca.org/).

• *Questionnement systématique*

Dans tous les cas, on s'assurera que le PSI traite les questions suivantes :

- Pourquoi cela doit-il être fait ?
- Comment cela doit-il être fait ?
- Qui doit le faire ? On s'interrogera notamment sur le rattachement du responsable du PSI : est-il un des responsables de la Direction Informatique ou un des prestataires externes pilotés par la Direction Informatique ?
- Que doit-on faire ?
- Quand cela doit-il être fait ?
- Où cela doit-il être fait ?
- En suivant quelles politiques, règles, procédures ?
- Qui peut changer le plan et en quelles circonstances ?
- Sous quelles conditions un sinistre est-il déclaré terminé ?

© IFACI

2. *Les conseils normatifs de l'ISACA*

De son côté, l'IS Auditing Guideline G32 « Business continuity plan review from IT perspective » de l'ISACA précise les activités d'audit à réaliser selon les 3 aspects :

- organisationnel, en s'assurant par exemple qu'un budget est disponible et suffisant pour les tests, la mise en œuvre et la maintenance du PSI ;
- planifiable, en vérifiant par exemple qu'une analyse des risques et une analyse d'impact ont précédé la mise en place du PSI, ou encore que l'analyse des risques est revue périodiquement ;
- procédural, en s'assurant par exemple que les procédures adéquates d'urgence sont en place et testées, que les sauvegardes sont identifiables, que les résultats des tests du PSI sont documentés…

3. *Une autre démarche possible*

Anantha Sayana, dans son article « Auditing business continuity » paru dans Information system control journal, volume 1, 2005, propose une démarche d'audit en trois étapes :

- ***Valider le PSI :***
  - en contrôlant si le plan couvre tous les systèmes critiques de l'entreprise ;
  - en vérifiant si le plan est basé sur une analyse d'impact systématique qui prend en compte les conséquences d'indisponibilité des systèmes sur les intérêts vitaux de l'entreprise ;
  - en déterminant si le plan offre une combinaison pertinente de contrôles préventifs (face aux risques gérables) et de dispositifs de reprise (en tenant compte des DMIA et des PMDA) ;
  - en s'assurant que le PSI est mis a jour régulièrement et corresponde aux enjeux et risques de l'entreprise ;
  - en contrôlant la qualité des tests du PSI ;
  - en s'assurant que le PSI couvre non seulement la reprise après sinistre mais aussi la réinstallation éventuelle dans les locaux initiaux.
- ***Examiner les mesures préventives et autres permettant d'assurer la continuité :***
  - en vérifiant l'existence et le fonctionnement correct des contrôles préventifs ;
  - en appréciant la sécurité physique et logique du site de secours et son éloignement tant du site primaire que des locaux de stockage des sauvegardes ;
  - en s'assurant que les équipements et services logistiques (fluides, liquides, énergies...) sont en état de fonctionnement et qu'ils permettent, le cas échéant, la mise en œuvre de dispositifs redondants ;
  - en s'assurant de la redondance sécurisée des liaisons réseau tant du site primaire que du site de secours.
- ***Apprécier la performance des activités assurant la continuité et la reprise des activités :***
  - en examinant la qualité des back-up (conformité aux besoins et spécifications,

© IFACI

périodicité, "exploitabilité", degré de couverture, réalisation de tests ...) par échantillonnage de supports de sauvegarde ;
- en vérifiant les logs à l'issue des mécanismes de réplication des informations et en s'assurant que les sauvegardes réalisées sont compatibles avec le PMDA prévu et que les envois vers le site de sauvegarde le sont à intervalle compatible avec le DMIA ;
- en s'assurant de l'efficacité des contrôles par la lecture des logs de test et de maintenance de tous les équipements de sécurité (générateurs électriques, air conditionné, équipement de détection et d'extinction incendie...) ;
- en appréciant la complétude et la couverture des tests du PSI, ainsi que des retours d'expérience effectués à l'issue des tests ;
- en vérifiant que l'accompagnement des ressources humaines est effectif (sensibilité, formation, entraînement).

4. *L'approche CobIT*

Dans le cadre d'audits détaillés, CobIT fournit un cadre complet d'intervention sur le processus informatique DS4 - Assurer un service continu - suivant la démarche standard préconisée par ce référentiel :

- acquérir une bonne compréhension du processus, listant les personnes à interroger et les documents à obtenir ;
- évaluer les contrôles en vérifiant, par exemple, si les politiques et procédures des technologies de l'information prévoient :
  - un cadre et un environnement de contrôle cohérents pour l'élaboration d'un plan de secours ;
  - des priorités de reprise et de retour à la normale pour chaque application ;
  - l'évaluation des risques et une assurance en cas de pertes d'exploitation pour la fonction informatique et pour les utilisateurs de ressources ;
  - un aperçu des rôles et responsabilités spécifiques dans la planification de la continuité, qui intègre les besoins spécifiques en matière de test, de maintenance et de mise à jour ;
  - une formalisation des contrats passés avec les fournisseurs de prestations en cas de besoin de recours, incluant des accès ou des contacts avec le site de secours, avant d'en avoir réellement besoin.
- évaluer la conformité en s'assurant que, par exemple :
  - une formation et une sensibilisation des utilisateurs et du personnel de la fonction informatique ont eu lieu pour définir les tâches et les responsabilités spécifiques qu'ils doivent assumer dans le cadre du plan ;
  - les relations avec les prestataires sous contrat et les délais de livraison et mise en place sont cohérents avec les attentes et les impératifs des utilisateurs ;
  - tout ce que contient le site de secours est à jour, adéquat et conforme aux procédures de rotation hors site.
  - les données et les opérations critiques ont été précisées, identifiées et documentées ;
  - la Direction Générale donne son aval sur la criticité des données et des opérations.

© IFACI

- apprécier le risque de ne pas atteindre les objectifs détaillés, en effectuant, par exemple, un examen détaillé :
  - à partir d'entretiens de personnes sélectionnées au sein de la fonction informatique et des services utilisateurs pour s'assurer que les impératifs de l'activité sont pris en compte dans le plan de secours ;
  - des procédures alternatives de traitement manuel des données par les utilisateurs jusqu'a la reprise de l'exploitation normale.

  En identifiant, par exemple :
  - l'existence, dans le plan, de divers scénarios allant des coupures temporaires à l'arrêt à durée indéterminée ;
  - l'affectation des priorités aux applications pour s'assurer qu'elle est cohérente avec l'attente des utilisateurs ;
  - l'adéquation des équipements informatiques du site de secours aux besoins en vérifiant qu'elle est garantie par des contrats écrits ;
  - l'adéquation, sur le site de secours, de la vitesse d'exécution, du temps de réponse, de la disponibilité et du support par rapport aux impératifs des utilisateurs.

On peut aussi reprendre de manière interrogative les objectifs de contrôle détaillés énumérés dans DS4, ce qui permet, par exemple, d'obtenir le questionnaire suivant :

- **Thème « Plan de secours informatique » :**
  Le management de la fonction informatique a-t-il créé un cadre de continuité qui définit les rôles et les responsabilités, la démarche ou la méthodologie à adopter, les règles et les structures pour documenter le plan, ainsi que les procédures d'approbation ?
- **Plan de secours informatique : stratégie et philosophie**
  Le management s'assure-t-il que le plan de secours est en ligne avec le plan de continuité d'entreprise de manière à en garantir la cohérence ?
  Le management s'assure-t-il que le plan de secours se conforme au plan de continuité d'entreprise dans le cadre des dispositifs de communication (par exemple avec les media en cas de crise) ?
  Le plan de secours informatique prend-il en compte le plan informatique à moyen et long terme pour en garantir la cohérence ?
- **Contenu du plan de secours informatique :**
  Le management de la fonction informatique s'assure-t-il qu'un plan écrit est élaboré et contient les rubriques suivantes :
  - documentation sur le mode d'emploi du plan de secours ;
  - procédures d'urgence pour assurer la sécurité de tous les membres du personnel touchés ;
  - procédures de réaction face à l'incident ou au sinistre ;
  - procédures de restauration destinées à remettre l'entreprise dans l'état où elle était avant l'incident ou le sinistre ;
  - procédures de sauvegarde et de reconstruction du site, procédures de coordination avec les autorités publiques ;
  - procédures de communication avec les parties prenantes : employés, principaux clients, fournisseurs critiques, actionnaires et management ;

© IFACI

- informations cruciales sur les équipes de continuité, le personnel concerné, les clients, les fournisseurs, les autorités publiques et les médias.

- **Minimiser les besoins de secours informatique :**
  Le management de la fonction informatique a-t-il défini des procédures et des guides pour réduire les besoins de continuité en matière de personnel, d'installations, de matériels, de logiciels, d'équipements, d'imprimantes et de mobilier ?
- **Maintenance du plan de secours informatique :**
  Le management de la fonction informatique a-t-il mis en place des procédures de contrôle des modifications pour s'assurer que le plan de secours est à jour et reflète les besoins réels de l'entreprise ? (procédures de maintenance du plan de secours en ligne avec les procédures en matière de modification, de gestion et de ressources humaines)
- **Test du plan de secours informatique :**
  Le management évalue-t-il périodiquement la pertinence du plan de secours ? (comment, quelle formalisation, quelle suite en est donnée ? Obtenir des éléments tangibles)
- **Formation au plan de secours informatique :**
  La méthode suivie pour assurer la continuité après un sinistre prévoit-elle que toutes les parties concernées bénéficient de sessions de formation périodiques sur les procédures à suivre en cas d'incident ou de sinistre ?
- **Diffusion du plan de secours informatique :**
  Le plan de secours n'est-il diffusé qu'auprès des personnes autorisées et est-il protégé de tout risque de diffusion non autorisée ?
- **Procédures alternatives de traitement pour le secours des départements utilisateurs :**
  La démarche suivie permet-elle d'assurer que les départements utilisateurs mettent en place des procédures alternatives de traitement qui peuvent être utilisées jusqu'à ce que la fonction informatique soit en mesure de restaurer entièrement ses services après un sinistre ?
- **Ressources informatiques critiques :**
  Le plan de secours identifie-t-il les programmes d'applications critiques, les services de tiers, les systèmes d'exploitation, le personnel et les fournitures, les fichiers de données et les délais nécessaires à la reprise après un sinistre ?
- **Site et matériel de secours :**
  S'assure-t-on que la démarche suivie comprend l'identification de sites et de matériels de secours alternatifs, ainsi que le choix final ?
- **Procédures d'évaluation après sinistre :**
  Après un sinistre, à la suite de la reprise avec succès des services informatiques, le management de la fonction informatique a-t-il défini des procédures pour évaluer l'adéquation du plan et le mettre à jour en conséquence ?

Il est aussi recommandé de ne pas se cantonner à la revue du seul PSI, mais de s'intéresser à l'environnement de pilotage et de sécurité. Dans ce cas, il pourra être particulièrement intéressant de regarder plus spécifiquement d'autres processus CoBit (4.0) :

© IFACI

- PO6 : faire connaître les buts et orientations du management,
- PO9 : évaluer et gérer les risques,
- DS1 : définir et gérer les niveaux de service,
- DS5 : assurer la sécurité des systèmes,
- DS11 : gérer les données,
- DS12 : gérer l'environnement physique,
- SE2 : surveiller et évaluer le contrôle interne,
- SE3 : s'assurer de la conformité réglementaire,
- PO8 : gérer la qualité,
- DS2 : gérer les services tiers.

On pourra aussi, plus accessoirement, s'intéresser à des parties des processus :

- PO8 : gérer la qualité,
- AI6 : gérer les changements,
- DS9 : gérer la configuration,
- DS10 : gérer les problèmes,
- DS13 : gérer l'exploitation.

© IFACI

6- Assurance et audit de PCA

1. *Audit des contrats d'assurance*

Quelles sont les garanties qui couvrent une interruption ou une baisse d'activité ?

- Distinguer parmi les contrats souscrits ceux qui concernent la continuité d'activité.
- Classer les garanties par grande catégorie :
  - pertes d'exploitation ;
  - frais supplémentaires ;
  - frais supplémentaires additionnels ;
  - extension de garantie.

Comment vont jouer les garanties en cas de sinistre ?

- Analyser les garanties :
  - faits générateurs ;
  - objets de risques concernés ;
  - exclusions ;
  - franchises et plafonds.

2. *Audit de la valorisation des ressources utilisées en PCA*

Quelles indemnités d'assurance seront perçues en cas de sinistre ?

- Ne tenir compte que des événements aléatoires.
- Calculer les indemnités :
  - selon différents scénarios d'indisponibilité (étendue, durée) ;
  - en tenant compte des franchises et plafonds ;
  - sur la base des dépenses internes ou externes justifiables.

5. *Audit de la révision des garanties*

Quelle est la fréquence de mise à jour des contrats ?

- Ne pas laisser les contrats plus de trois ans sans en faire la revue.
- Revoir les garanties lors des changements importants affectant l'entreprise (techniques, logistiques, organisationnels).

6. *Audit de la sécurité des archives*

Quelle protection est en place ?

- La garantie prévoit le remboursement des frais de reconstitution des informations à partir d'un support existant.
- Vérifier que des copies des archives existent pour que la garantie joue.

© IFACI

7. *Audit du PCA du sous-traitant*

Que couvrent les contrats d'assurance souscrits par le sous-traitant ?

- Vérifier si des garanties concernent la continuité de la prestation achetée.
- Vérifier que le sous-traitant peut surmonter une interruption ou une baisse de son activité.

Que couvre le PCA du sous-traitant ?

- Vérifier si le plan couvre la continuité de la prestation achetée.
- Participer aux tests du PCA du sous-traitant.
- Prévoir la possibilité d'audit de la prestation chez le sous-traitant.

© IFACI

7- Référentiel de bonnes pratiques : communication interne, formation et PCA

1. *PCA et Communication interne*

Le Plan de continuité d'activité doit faire l'objet d'une communication interne régulière dès le début de sa conception. Le personnel doit comprendre que le PCA est la volonté de la Direction Générale et qu'il **s'agit d'un projet qui concerne toute l'entreprise aujourd'hui et pour longtemps.**
L'information du personnel est indispensable pour éviter une mauvaise compréhension du PCA et notamment pour répondre à certaines questions que se pose le personnel et aborder au moins les notions suivantes :

- Qu'est-ce que le PCA (enjeux, objectifs, périmètre couvert, solutions pour assurer la continuité) ?
- Qu'est-ce qu'une activité critique ?
- Pourquoi l'entreprise ne peut elle pas prévoir un site de repli pour héberger tout le personnel ?
- Le personnel non impliqué sur le site de repli percevra-t-il la totalité de son salaire s'il ne travaille pas sur les sites de repli ?
- Quelle est l'organisation du travail sur le site de repli (horaires, transport, restauration…) ?…

Il convient de prévoir un accès aux informations adapté au personnel des activités non définies comme critiques.

Le contenu de l'information est défini par le responsable du projet PCA en accord avec la Direction Générale. Différentes formes et supports de communication peuvent être utilisés:

- lettre de la Direction Générale à l'ensemble du personnel lors du lancement du projet ;
- présentation du projet PCA et points d'avancement devant les instances représentatives (CE, DP…) du personnel et le CHSCT (Comité d'Hygiène, de Sécurité et des Conditions de Travail). Un point trimestriel est recommandé et au moins lors des étapes suivantes :
  - définition de la stratégie de continuité et choix de(s) site(s) de repli. Une visite du ou des site(s) de repli avec un représentant du CHSCT est fortement recommandée ;
  - finalisation de la rédaction des procédures PCA ;
  - formation des équipes impliquées sur le site de repli ;
  - choix de la date du test annuel impliquant le personnel et présentation de l'organisation de la journée de test.
- informations sur l'évolution du projet PCA sur un site intranet créé spécifiquement pour informer le personnel sur le PCA. Ce site peut ensuite évoluer pour devenir plus tard le lieu de conservation des procédures et autres documents qui matérialisent le PCA ainsi qu'un lieu interactif où le personnel peut poser des questions sur le PCA ou l'organisation des tests ;

© IFACI

- communication de la Direction Générale pour entériner l'existence du PCA (site de repli validé techniquement, procédures écrites) ;
- communication de la Direction Générale annonçant la phase de formation du personnel impliqué sur le(s) site(s) de repli ;
- communication de la Direction Générale annonçant le test annuel du PCA impliquant le déplacement du personnel sur le site de repli (date/organisation) ;
- communication de la Direction Générale remerciant le personnel après le test et donnant les résultats du test.

2. *PCA et Formation du personnel impliqué sur le site de repli*

Le personnel impliqué sur les sites de repli, doit recevoir une formation spécifique. Le personnel formé est celui dont les noms figurent dans les procédures métiers ou fonctions.
La formation doit être effectuée de préférence par le responsable du PCA ou toute personne ayant suffisamment de connaissances pour répondre aux questions des participants.
Un sponsor (DRH, directeur métier, membre de la Direction) est recommandé pour initier les 5 premières minutes de la formation.
La formation doit être réalisée par métier ou par fonction avec un maximum de 20 personnes par session pour favoriser les échanges.
La formation est souvent la seule opportunité de répondre aux questions du personnel avant la réalisation du premier test impliquant les métiers et les fonctions sur le site de repli.
La formation se déroule sur une demi-journée. Sa durée varie entre 2 ou 3 heures selon la complexité de la stratégie de continuité et le nombre de participants.
La formation doit au moins couvrir les points suivants :

- **l'explication de la stratégie de continuité des activités :**
  - le choix des activités critiques ;
  - les impacts d'une interruption du service ou de la fonction concernée sur l'entreprise ;
  - le délai maximum d'interruption admissible ;
  - le niveau de service ou de production que le service ou le métier doit assurer depuis le site de repli ;
  - les ressources humaines et matérielles prévues pour chaque service ou métier.
- **la présentation du site de repli**
  - localisation, plan d'accès, photos du site de repli ;
  - emplacement, plan d'installation des services sur le site de repli ;
  - moyens de transport prévus ;
  - organisation du site (sécurité, heures d'ouverture, règles de fonctionnement).
- **la rémunération associée au PCA**
  - remboursement de frais ;
  - primes éventuelles.

© IFACI

- **les processus d'activités détaillés du service ou du métier**
  - selon les services/métiers ;
  - objectifs et utilisation des journaux de bord.
- **la vie du dossier PCA**
  - tests ;
  - mises à jour des procédures.

Seules les personnes ayant participé à la formation peuvent être ensuite sollicitées pour effectuer les tests sur le site de repli.
Chaque année une session de formation doit être réalisée après la mise à jour du PCA.
Le nouveau personnel dont le nom est inclus dans la mise à jour des procédures métiers et fonctions doit participer à ces sessions de formation.

© IFACI

8- CHARTE DU PCA

Axes de réflexion pour élaborer et déployer une charte de gestion et de contrôle du plan de continuité d'activité.

1. *Objectifs :*

Cette charte a pour objectif de « **faire vivre l'esprit de continuité** » initié lors du projet. Elle doit faciliter le dialogue entre acteurs du plan de continuité d'activité.
En s'intéressant à la pérennité des activités, elle prend **sa place dans l'économie générale du système de contrôle interne.**
Elle peut être déployée, sous l'impulsion de la Cellule de Crise Décisionnelle, pour décrire les obligations et l'environnement de contrôle nécessaires au bon fonctionnement du maintien en condition opérationnelle du plan de continuité d'activité **dans le respect de la culture d'entreprise.**
Cette charte prend en compte les règles fixées par les lois, décrets, règlements et obligations imposés par les législateurs, les régulateurs, la maison mère et/ou l'organe central et les bonnes pratiques professionnelles.

2. *Principes :*

La charte est mise en œuvre, **dans le cadre du système de contrôle interne de l'entreprise**, pour encadrer le plan de continuité des activités et définir ses modalités pratiques de maintien en condition opérationnelle.
Elle confirme la nécessité de prendre en compte la continuité d'activité dans les nouveaux projets et développements.
Elle impose une fréquence de révision et de validation du périmètre :

- la charte est présentée aux organes de gouvernement d'entreprise qui la valident ;
- la fréquence et les modalités de révision de la charte sont précisées.

Elle définit les modalités de désignation et de rattachement du RPCA.

3. *Champ d'application*

La charte se rapporte à l'ensemble des activités internes et externes de l'entreprise.
Elle concerne toutes les entités juridiques de l'entreprise (tête de groupe, filiales).
Elle s'intéresse à la couverture de la continuité d'activité en terme de scénarios.
La charte garantit la conformité des relations contractuelles entre l'entreprise et des prestataires externes concernés par la continuité d'activité ou fournisseurs de prestations essentielles.
Elle garantit la prise en compte de la continuité d'activité dans la cartographie des risques et la gestion des risques opérationnels

© IFACI

4. *Acteurs*

Il convient de définir précisément le rôle de chacune des instances :

- Conseil d'Administration / Conseil de Surveillance ;
- Direction Générale ;
- Cellule de Crise Décisionnelle ;
- Comité d'Audit, Commissaires aux Comptes ;

Il convient de définir précisément le rôle et le positionnement de chacun de ces intervenants :

- Responsable du Plan de Continuité d'Activité (RPCA) ;
- Correspondants Continuité d'Activité (CCA) ;
- Risk Manager, Responsable des Risques Opérationnels ;
- Responsable de la Sécurité du Système d'Information ;
- Responsable du Plan de Secours Informatique...

5. *Contrôle Interne*

Il convient de définir précisément le rôle des différents niveaux de contrôle en fonction de l'organisation de l'entreprise :

- mise à l'ordre du jour des comités de contrôle ;
- modalités de révision des documents essentiels ;
- conservation et accessibilité des documents essentiels de gestion du PCA ;
- révision des modalités contractuelles et d'assurance ;
- intégration dans le dispositif de contrôle interne ;
- inscription au plan d'audit.

6. *Tests et exercices*

Ce chapitre s'intéressera aux opérations suivantes :

- validation des programmes ;
- intervention des prestataires (ressources humaines, locaux, support logiciel …) ;
- inscription au planning ;
- reporting.

7. *Information*

On définira l'organisation des items suivants :

- communication interne, externe (clients, fournisseurs...) ;
- supports autorisés (internet…) ;
- diffusion d'un tableau de bord ;
- rapports annuels (réglementaires, gestion, moral…).

© IFACI

8. *Formation / Sensibilisation*

On indiquera les modalités de réalisation et d'actualisation des actions de formation et de sensibilisation pour :

- la cellule de Crise Décisionnelle,
- le RPCA / les CCA,
- les collaborateurs.

9. *Budget*

On précisera les modalités de déclaration d'engagement budgétaire en adéquation avec les efforts demandés par la continuité d'activité (ressources humaines, matérielles, technologiques, logicielles,…).

10. *Dossiers liés*

On veillera à identifier :

- tout document encadrant la gestion de crise ;
- le système de délégations de pouvoirs de l'entreprise.

© IFACI

9- « FEUILLE DE ROUTE » DU RPCA

Ce que peut contenir la « feuille de route » du Responsable du Plan de Continuité d'activité :
Comme le précise la lettre de mission du RPCA, il a pour rôle d'assurer la réalisation du PCA, et doit avoir la capacité à mobiliser les ressources et moyens humains et financiers nécessaires tant dans la phase projet que dans la phase maintien en condition opérationnelle.
Pour atteindre ces objectifs, le RPCA doit engager les principales actions suivantes :

1. Sensibiliser les acteurs majeurs et indentifier les attentes de la Direction Générale

Le PCA est un processus permanent qui nécessite un plan d'actions annuel proposé par le RPCA :

- sensibiliser la Direction Générale et les responsables des Filières ou Services au PCA à l'aide de la présentation méthodologique retenue et avec l'appui de la direction de projet Groupe si besoin est ;
- porter son plan d'actions à la connaissance de la Direction Générale et faire valider les moyens nécessaires à sa réalisation et à la hauteur des objectifs fixés ;
- insister sur le fait que le PCA ayant pour but d'assurer la continuité de l'ensemble des activités d'une entreprise en cas de sinistre majeur, son élaboration et son maintien opérationnel mobilisent donc toutes les Filières ou Services ;
- organiser un programme de sensibilisation voire de formation pour l'ensemble des collaborateurs de l'entreprise.

2. Mettre en place une organisation de projet et piloter le projet

Le grand nombre d'acteurs impliqués et de tâches à mener obligent à :

- mettre en place une organisation de projet (comité et direction de projet),
  - le RPCA doit s'appuyer sur des correspondants qui, selon le cas, sont amenés à réaliser eux-mêmes une partie du PCA ou à s'appuyer sur des experts métiers ou techniques pour le mettre en œuvre. Lorsque des experts sont mobilisés, le RPCA et les correspondants PCA auront essentiellement pour rôle de sensibiliser, coordonner et animer les travaux. Dans tous les cas, le RPCA validera l'ensemble des plans rédigés.
- découper le projet en lots, chaque lot comprenant une phase de conception, de réalisation, de test et de recette,
- un premier niveau de découpage du PCA consistant à distinguer le plan global de gestion de crise, les plans de continuité au niveau de chacune des filières ou services et les quatre plans transverses (Communication, Ressources Humaines, Systèmes d'Information, Logistique et Sécurité). Le RPCA pourra affiner la rédaction des plans en complétant avec des solutions pour assurer la continuité des activités. Il en résulte des lots ou projets complémentaires dont certains devront se dérouler en parallèle et pour lesquels le RPCA devra veiller à leur réalisation et à leur conformité avec les besoins exprimés.

© IFACI

- définir les livrables et le planning de chaque lot, en veillant à un avancement homogène et parallèle des plans, pour faciliter les tests, garantir la résilience et limiter le projet dans le temps.
- suivre régulièrement l'avancement du projet, en mettant en place un tableau de bord.

3. *Définir et mettre en place une organisation de gestion de crise, élaborer le plan de gestion de crise*

- installer l'organisation de gestion de crise qui pilotera les opérations lors d'un sinistre consiste à :
  - mettre en place la CCD (Cellule de Crise Décisionnelle) : désignation des membres et définition du mode de fonctionnement général,
  - créer les CCO (Cellules de Crise Opérationnelles) au niveau des filières ou services où cela apparaît nécessaire, et définir leur mode de fonctionnement interne et avec la CCD.
- élaborer le plan de gestion de crise ;
  - en rédigeant :
    - les procédures de remontée d'alerte,
    - les procédures de déclenchement du PCA,
    - les procédures de gestion de crise.
  - en créant les mallettes de crise ;
  - en testant son efficacité (test de repli de la CCD ou test de tout ou partie d'un des scénarios du guide).

4. *Faire engager les actions pour rendre les plans de continuité opérationnels*

Déclencher un plan de continuité, c'est entrer dans une gestion dégradée des activités avec des ressources limitées, éventuellement autres que les moyens habituels, et dans un environnement qui peut être différent de celui d'origine. C'est mettre en place des mesures de :

- secours (repli des collaborateurs, backup des systèmes d'information) ;
- contournement (accords particuliers, solutions alternatives, etc.) ;
- continuité (reprise des activités de manière dégradée, etc.).

Si l'entreprise ne dispose pas des moyens nécessaires, le RPCA va devoir engager des plans d'actions pour les rendre disponibles le moment venu. Ces plans d'actions résultent de l'analyse des écarts entre les besoins exprimés et les services offerts. En outre, l'élaboration des plans pourra être l'occasion de lancer ou de renforcer des mesures de prévention pour diminuer la probabilité de survenance d'un sinistre ou en réduire l'impact (mise en sécurité des immeubles, sûreté de fonctionnement, sécurité des systèmes d'information, sécurité des personnes et des biens, prise en compte du PCA dès la conception de nouveaux projets ...).

Parmi les mesures de prévention, figurent aussi l'examen des relations avec les tiers qui doit conduire à formaliser les accords avec les prestataires internes ou externes

© IFACI

(engagements contractuels des fournisseurs et partenaires en cas de sinistre chez le prestataire ou de sinistre touchant l'entreprise).

Il en résulte des coûts, des investissements et des projets connexes au PCA que le RPCA devra faire arbitrer par la Direction Générale.

5. Tester et maintenir en condition opérationnelle

Le projet PCA est réputé achevé lorsque l'ensemble de ses composants a été testé. Il appartient au RPCA, en relation étroite avec les filières ou services et l'organisation de crise, de préparer les tests, de les dérouler, d'en valider les résultats et de suivre les actions correctrices nécessaires.

Le maintien en condition opérationnelle du PCA est un processus permanent. Il doit être effectué une à deux fois par an et, à chaque évolution importante des activités ou des moyens, pour éviter son obsolescence. Le RPCA anime cette maintenance et en rend compte. Tous les comptes-rendus et fiches de test datées et signées, devront être archivés comme élément de preuve vis-à-vis du contrôle interne et des autorités de tutelle. Des tests réguliers restent là aussi la meilleure façon de garantir le caractère opérationnel des plans.

© IFACI

10- Bilan d'impact sur activités du PCA

		Date de MAJ :	
		Référence BIA :	
IDENTIFICATION			
		Criticité	**DMIA**
Process Essentiel			
Flux moyen			
Personnel concerné		Equivalent temps plein	
			Flux moyen
Sous Process 1			
Sous Process 2			
Sous Process 3			
Sous Process 4			

© IFACI

CONTACTS		
Responsables d'activités :		
Tél. Bureau :	**Tél. Domicile :**	**Portable Perso :**
Adresse bureau : Etage : Bureau :	Adresse domicile :	
Tél. Bureau :	**Tél. Domicile :**	**Portable Perso :**
Adresse bureau : Etage : Bureau :	Adresse domicile :	
Adresse bureau : Etage : Bureau :	Adresse domicile :	
Personne clé :		
Tél. Bureau :	**Tél. Domicile :**	**Portable Perso :**
Adresse bureau : Etage : Bureau :	Adresse domicile :	

© IFACI

INCIDENCES SUR LE SCHÉMA DE CIRCULATION FONCTIONNEL		
Processus Amonts :	Activité(s) :	Processus avals :

LOCALISATION (en période habituelle)			
Adresse :		Etage :	Bureau :
Tél. :	Fax :	Mail de service :	

MODALITÉS DE REPLI DES COLLABORATEURS					
Lieu	**Chronologie**				
	> 1 J	**< 5 J**	**< 10 J**	**< 15 J**	**> 1 M**
< Autre lieu 1 >					
< Autre lieu 2 >					

RISQUE / IMPACT	
Risque d'image :	
Résumé d'impact :	
Sensibilité saisonnière :	
Impacts réglementaires :	
Impacts partenaires :	
Impacts adhérents :	

© IFACI

IMPACT FINANCIER

Durée de l'interruption	Perte de chiffre d'affaires (euros)	Impact sur l'image oui/non et/ou (euros)	Impact total
Inférieur à 1 jour			
1 jour			
2 jours			
3 jours			
4 jours			
5 jours			
10 jours			
15 jours			
20 jours			

LISTE DES APPLICATIONS INFORMATIQUES ESSENTIELLES À L'ACTIVITÉ

Noms des applications informatiques	Lieu d'hébergement habituel	Lieu du Back Up

Autres Spécificités et Besoins Techniques ou Technologiques	
Postes Spécifiques :	
Accès Réseau Spécifique :	
Autres :	

POINTS ESSENTIELS DE LA PROCÉDURE DE CONTOURNEMENT

© IFACI

11- Questionnaire d'auto - évaluation du Plan de Continuité d'Activité (PCA)

A - Méthodologie et présentation générale

Un guide méthodologique a-t-il été utilisé pour l'élaboration et la mise en place du PCA au sein de la société ? De quelle nature de référentiel s'agit-il ?
Qui a été associé au choix du guide méthodologique pour élaborer le PCA ?
Quels sont les scénarios pris en compte dans l'élaboration du PCA ?
L'entreprise a-t-elle recensé les prestataires essentiels à son activité qui sont impactés par l'élaboration de son PCA ?
La continuité des prestations essentielles sous-traitées est-elle assurée pour l'ensemble des prestataires ou à défaut, par l'entreprise ?

B - Organisation et structures

Un responsable du plan de continuité d'activité (RPCA) a-t-il été désigné au sein de l'entreprise ? Dispose-t-il d'une fiche de poste ou d'une lettre de mission ?
Un suppléant du RPCA a-t-il été nommé ? Dispose-t-il d'une fiche de poste ou d'une lettre de mission ?
Un plan de Gestion de Crise a-t-il été formalisé ?
Une Cellule de Crise Décisionnelle (CCD) a-t-elle été constituée au sein de l'entreprise ?
Le RPCA est-il l'animateur de la Cellule de Crise Décisionnelle ?
Des Cellules de Crise Opérationnelles (CCO) ont-elles été mises en place ?
Des Correspondants de ces Cellules de Crise Opérationnelles ont-ils été désignés ?
Le Plan de Gestion de Crise (PGC) comprend-il une (ou des) procédure (s) de remontée d'alerte ?
Cette procédure comprend-elle un schéma de remontée d'alerte opérationnelle prenant en compte un traitement différencié selon le type de scénario, le moment de survenance du sinistre, l'ampleur du sinistre et selon l'organisation de l'entreprise ?
Le Plan de Gestion de Crise comprend-il les procédures de déclenchement du PCA ?
A–t-il été validé par le RPCA ?
Les plans de gestion de crise par domaine d'activité ou transversaux ont-il été validés par le RPCA ?
Le Plan de Gestion de Crise a-t-il été présenté à la Cellule de Crise Décisionnelle ?
Le Plan de Gestion de Crise a-t-il été validé par la Cellule de Crise Décisionnelle ?
Le Plan de Gestion de Crise prévoit-il l'existence de mallettes de crise? Le contenu des mallettes est-il détaillé ?

© IFACI

C - Analyse des besoins et des solutions

C-1- Référentiel Existant et Besoins (REB)

Le recensement des activités a-t-il été réalisé sur la base d'un référentiel (exemple : référentiel des domaines et sous domaines de la gestion des risques opérationnels) ?
L'ensemble des éléments suivants ont-ils été intégrés au référentiel :

- service ou unité de traitement ;
- effectif ;
- dénomination ;
- le Délai Maximum d'Interruption Admissible (DMIA) ;
- les besoins en continuité (DMID : Délai Maximum d'Indisponibilité Demandé) ;
- la criticité financière …

C-2- Bilan d'Impact sur Activités (BIA) et Synthèse BIA (SBIA)

L'entreprise a-t-elle établi un Bilan d'Impact sur Activités (BIA) par activité ?
Les Bilan d'Impact sur Activités ont-ils fait l'objet d'une validation par les responsables des activités concernées ?
Dans ces Bilans d'Impact sur Activités, un niveau de criticité par activité a-t-il été défini ?
Le niveau de criticité par activité dépend-il du délai maximum d'interruption admissible (DMIA) et/ou du niveau des pertes financières ?
Une synthèse des Bilans d'Impact sur Activités a-t-elle été élaborée? Classe-t-elle les activités par niveau de criticité ?

D - Plans et solutions de secours

D-1- Plans de Continuité des Entités de l'entreprise

Les entités de l'entreprise ont-elles été recensées ?
Les Plans de continuité des entités de l'entreprise sont-ils construits selon la méthodologie retenue par l'entreprise et notamment présentent-ils :

- une gestion par type de scénario ?
- une description des procédures de contournement et des moyens ou des solutions de secours à mettre en œuvre ?

Retrouve-t-on dans les Plans de continuité des entités de l'entreprise une synthèse des besoins propres exprimés par les entités concernées ?
Face aux besoins exprimés par l'entité concernée, trouve-t-on dans les Plans de continuité des entités de l'entreprise la déclinaison opérationnelle des moyens correspondants ?
Les Plans de continuité des entités de l'entreprise intègrent-ils les volets Communication, Ressources Humaines, Systèmes d'Information, Logistique, Sécurité ?

© IFACI

Le RPCA dispose-t-il d'une cartographie des activités et des applications lui permettant de vérifier l'interdépendance des Plans de Continuité des entités de l'entreprise entre chaque sous domaine d'activité?

D-2- Plan de Continuité Communication

Le Plan de Continuité Communication (PCC) de l'entreprise a-t-il été élaboré ?
Des messages types ont-ils été rédigés en fonction de la cible et de la phase de la crise (réaction, gestion en mode dégradé et retour à une situation normale) ?
Les outils de communication qui peuvent être utilisés dans le Plan de Continuité Communication ainsi que dans les différents plans transversaux ont-ils été identifiés et catégorisés ?
Le Plan de Continuité Communication prévoit-il, pour chacun de ces moyens : l'intervenant en charge de la communication, la manière de l'activer, la manière de le gérer, la fréquence de sa mise à jour et la technique d'alimentation des supports ?
Le Plan de Continuité Communication prévoit-il une liste prédéfinie de personnes habilitées pouvant communiquer vers l'extérieur en cas de crise (selon la nature et l'ampleur de la crise) ?

D-3- Plan de Continuité Ressources Humaines

Le Plan de Continuité Ressources Humaines (PCRH) a-t-il été rédigé ?
Des outils ont-ils été mis en place pour adapter les conditions de travail à la crise ?
Le Plan de Continuité Ressources Humaines intègre-t-il des procédures de gestion de crise impliquant la filière RH de l'entreprise (Gestion pendant la crise et accueil post-sinistre) ?
Les contrats de prestations de services (spécialement la mise en place de prestataires de service dans les équipes) prennent-ils en compte les situations exceptionnelles liées au PCA ?
La réglementation en matière de données nominatives (CNIL) a-t-elle été respectée lors de l'élaboration des listes et le recueil des coordonnées personnelles des collaborateurs et des personnes concernées ?

D-4- Plan de Continuité des Systèmes d'Information

Le Plan de Continuité des Systèmes d'Information (PCSI) a-t-il été élaboré ?
Le périmètre du Plan de Continuité des Systèmes d'Information couvre-t-il l'ensemble des Systèmes d'Information de l'entreprise ?
Le rôle des différents intervenants dans les solutions de continuité de service et leurs modalités de mise en œuvre sont-ils détaillés dans des engagements contractuels (convention, contrat…) ?
Retrouve-t-on dans le Plan de Continuité des Systèmes d'Information la description des besoins en matière d'équipements des sites de repli et des salles de réunion (infrastructure nécessaire au fonctionnement des systèmes d'information) ?
Trouve-t-on dans le Plan de Continuité des Systèmes d'Information une cartographie des Systèmes d'Information internes et externes ? Des schémas d'architecture des solutions de secours existent-ils ?

© IFACI

Les moyens et les procédures de secours techniques et opérationnels décrits dans le Plan de Continuité des Systèmes d'Information permettent-ils d'assurer :

- le secours du matériel informatique (serveurs, réseau,…) ?
- le secours des applications (y compris la sauvegarde des données) ?
- la mise en œuvre des moyens de contournement ?
- la gestion de la montée en charge et de la continuité d'activité ?

Les moyens de procédures de secours du site central informatique ont-ils été décrits ?

D-5- Plan de Continuité Logistique et Sécurité

Le Plan de Continuité Logistique et Sécurité (PCLS) a-t-il été élaboré ?
Le Plan de Continuité Logistique et Sécurité intègre-t-il un processus formalisé décrivant les interventions des fournisseurs et partenaires lors d'une crise dans l'entreprise ?
Le Plan de Continuité Logistique et Sécurité décrit-il le rôle de la Logistique et de la Sécurité :

- dans le schéma de remontée d'alerte ?
- dans l'accueil post-sinistre ?

Lors d'une crise, le Plan de Continuité Logistique et Sécurité prévoit-il :

- des mesures de gestion du courrier ?
- des mesures de gestion de la reprographie ?
- des mesures de gestion des approvisionnements ?
- des mesures de la gestion des documents ?

Le Plan de Continuité Logistique et Sécurité prévoit-il les modalités de la mise en œuvre et de la gestion des sites de repli et salles de réunion de crise ?

E - Maintien en condition opérationnelle

Existe-t-il un dispositif de Maintien en Condition Opérationnelle (MCO) formalisé, notamment des procédures de mise à jour du PCA ?
Des moyens nécessaires ont-ils été engagés pour mettre en œuvre ce dispositif de Maintien en Condition Opérationnelle ?
Les contrôles de second niveau du PCA sont-ils intégrés dans les contrôles permanents ?
Le thème du PCA est-il intégré dans les audits thématiques ou d'entités menés dans l'entreprise ?
Existe-t-il un calendrier de tests pluriannuels ?
L'entreprise dispose-t-elle d'un outil de gestion du PCA ?
Des moyens financiers spécifiques dédiés au PCA ont-ils été budgétés pour l'année en cours ?
Le PCA a-t-il fait l'objet d'une mise à jour depuis sa mise en place ?
Existe-t-il une procédure de mise à jour du contenu des mallettes (alimenter, maintenir, sécuriser les supports d'information,…) composant la boîte à outils du PCA ?
Le thème du PCA est-il intégré dans les audits thématiques menés dans l'établissement ?
Les organes de gouvernement de l'entreprise sont-ils informés des modifications intervenues sur le PCA ?

© IFACI

© IFACI

BIBLIOGRAPHIE

- Catastrophe et management - Plans d'urgence et continuité des systèmes d'information - Daniel Guinier, Masson, 1995
- Plan de Continuité d'Activité et Système d'Information : vers l'entreprise résiliente - Matthieu Bennasar, Dunod, 2006
- Dispositif de gestion de continuité - PRA/PCA : une obligation légale pour certains et un impératif pour tous - Daniel Guinier, Revue Expertises, No.308, Nov. 2006, pp.390-396
- Plan de Continuité d'Activité et Système d'Information : vers l'entreprise résiliente - Matthieu Bennasar, Dunod, 2006
- Livre blanc : les éléments à intégrer dans un PCA pour gérer des chocs extrêmes – Romain Louzier, oct. 2005
- Principes directeurs en matière de continuité (Le Forum Tripartite) – the joint forum, Août 2006
- Revue BANQUE : continuité d'activité – fév. 2007
- Qualification de PCA – 2006
- norme BS 25999 : norme internationale en gestion de la continuité – 2006
- Audit check list – BS 7799-2 (British Standards) – 2002
- PAS 56 (Publicity Available Specification 56) : Guide to Business Continuity Management – ATSEC Information Security Corporation – 2003
- FSA – BCM – Practice Guide – nov. 2006
- Le management des risques de l'entreprise (cadre de référence – techniques d'application) COSO II report 2005
- Mémoire : audit d'un processus de gestion de crise – Thierry MERCIER (IFACI) 2000
- Mémoire : audit de la gestion de crise et du plan de continuité – Marianne KARDASZ (IFACI) 2003

- Outils et logiciels de traitement d'un PCA - Sites utiles :

  - GTAG 10 : Business Continuity Management
  - Outil Logiciel spécialisé dans la Gestion, le Maintien ainsi que la gestion de Crise d'un PCA édité par BCCM Strategy
  - Outil Logiciel de gestion d'un Plan de continuité (PCA) édité par eBRP
  - Outil Logiciel de gestion d'un Plan de continuité (PCA) édité par Sungard
  - Outil Logiciel de gestion d'un Plan de continuité (PCA) édité par Tamp et présenté en France par Expertilog
  - Outil Logiciel de gestion d'un Plan de continuité (PCA) édité par Strohl
  - Outil Logiciel de gestion d'un Plan de continuité (PCA) édité par devoteam
  - PCA par le CLUSIF

© IFACI

Réalisation : Ebzone Communication (ebzone@ebzone.fr)
Impression : Compédit Beauregard S.A. - 61600 La Ferté-Macé
N° d'imprimeur : 4475

© IFACI