Référentiel
de bonnes pratiques

Plan de Continuité d'Activité (PCA)

Activity continuity plan (ACP)

AFNOR

http://www.afnor.org

Liens avec des documents existants

À la date de publication du présent document, il existe un projet international traitant du même sujet.

Avant-propos

Membres du Groupe de Travail AFNOR/PCA (PLAN DE CONTINUITE D'ACTIVITE AFNOR Z50P) ayant contribué à l'élaboration et à la validation du présent Référentiel

Président : M HAMON

Secrétariat : MLLE ARBOUY — AFNOR

MLLE	ARBOUY	AFNOR
M	LEGENDRE	AFNOR
M	FOSSE	ALMA CONSULTING GROUP
M	DE THORE	CIE IBM FRANCE
M	NICOLAS	CIE IBM FRANCE
M	MOLINES	CLUSIR NORD PAS-DE-CALAIS PICARDIE
M	JACQUES	CNPP ENTREPRISE
M	RIO	CNPP ENTREPRISE
M	BESNIER	CRÉDIT AGRICOLE SA
M	GUILLERM	DION DÉFENSE & SÉCURITÉ CIVILES
M	FERRACCI	DSI — DÉLÉGATION SYSTÈMES INFORMATION
M	PULA	ÉCUREUIL GESTION
MME	BONNE	EDF GDF DIT
M	SOUBELET	EDF GDF DIT
M	GEYRES	ERNST & YOUNG ET ASSOCIÉS
M	HAMON	EXEDIS
M	LE MOING	EXEDIS
M	LACOMBE	FIDENS
M	RICHY	FRANCE TELECOM
M	OPITZ	GESTION ET SERVICES GROUPE COFINOGA GIE
M	AUTRET	GROUPEMENT DES CARTES BANCAIRES «CB»
MME	DEMACHY	MICA
MME	KERIHUEL	SFR SI
M	GRALL	SGDN
M	HAELLING	SI-LOGISM
M	DELACOURT	SUNGARD AVAILABILITY SERVICES
MR	LISETTE	SUNGARD AVAILABILITY SERVICES
M	VERGELY	SUNGARD AVAILABILITY SERVICES
MME	JUANALS	UNIVERSITÉ DE LILLE 3
M	PERRIAULT	UNIVERSITÉ DE PARIS X

Remerciements particuliers à :

Bruno HAMON pour son travail d'éditeur de Projet, et à Maître Isabelle RENARD (VAUGHAN Avocats) pour son expertise juridique.

Table des matières

Page

Table des matières (fin)

Page

1 Préambule

Ce document sur les bonnes pratiques en matière de Plan de Continuité d'Activité (PCA) respecte la législation existante sur les plans d'urgence. En France, les plans d'urgence prévoient un ensemble de mesures à prendre et de moyens de secours à mettre en œuvre immédiatement pour faire face à des risques de toute nature. La Loi n° 87-565 du 22 juillet 1987 relative à l'organisation de la sécurité civile, à la protection de la forêt contre l'incendie et à la prévention des risques majeurs (JO du 23 juillet 1987), abrogée par la loi n° 2004-811 du 13 août 2004 de modernisation de la sécurité civile (JO du 17 août 2004), a pour objet «la prévention des risques de toute nature, l'information et l'alerte des populations ainsi que la protection des personnes, des biens et de l'environnement contre les accidents, les sinistres et les catastrophes par la préparation et la mise en oeuvre de mesures et de moyens appropriés relevant de l'État, des collectivités territoriales et des autres personnes publiques ou privées. Elle concourt à la protection générale des populations, en lien avec la sécurité intérieure au sens de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure et avec la défense civile dans les conditions prévues par l'ordonnance n° 59-147 du 7 janvier 1959 portant organisation générale de la défense.» (Article 1) [1)].

En France, la circulaire interministérielle du «Plan Orsec» [2)] du 13 septembre 2005, centrée sur l'organisation des secours aux niveaux géographiques du département et de la zone de défense, recense et structure la mise à disposition des moyens nécessaires au déclenchement et à la prise en charge financière des secours. Les moyens de secours sont déclinés sous la forme de différents plans de secours (plan rouge, plan blanc, plans «pirates» — Piratair, Piratox…, etc.), assimilés à des plans de continuité sous certains de leurs aspects.

Par rapport aux plans de secours et de continuité existants, en cours de production ou en projet dans des organisations publiques ou privées, ce recueil de bonnes pratiques permet de s'assurer de la bonne prise en compte des éléments essentiels et de la méthodologie à adopter.

Au niveau du dispositif de gestion de crise, il appartiendra à chaque entité d'inscrire au niveau de ses annuaires spécifiques (livret de crise) les coordonnées des différentes instances gouvernementales et/ou autorités compétentes déterminées par le degré de gravité de la crise (commune, département, zone de défense).

Le fait que certaines entreprises aient mis en place une organisation résistante tant du point de vue métier que du côté technique devient un argument concurrentiel non négligeable.

Voir en **annexe**, quelques chiffres et statistiques.

2 Objectifs et domaine d'application

Au quotidien l'entreprise est amenée à gérer des situations imprévues pouvant avoir des conséquences sur son activité métier et lui entraîner des pertes d'exploitation. Les causes et impacts sont multiples allant de la destruction de ses locaux en passant par des défauts de production entraînant une perte d'image jusqu'à des cas extrêmes comme la pénurie de matières premières.

Dans le cadre de ses missions, le Groupe de Travail PCA a décidé de porter plus particulièrement son attention aux impacts d'une perturbation du système d'information de l'organisation sur son activité métier. D'ailleurs, la plupart des entreprises et des organisations ont mis en œuvre, se préparent à mettre en œuvre, ou font évoluer un Plan de Continuité d'Activité (PCA).

---

1) Loi n° 2004-811 du 13 août 2004, Loi de modernisation de la sécurité civile, Publication au JORF du 17 août 2004 [http://www.legifrance.gouv.fr/texteconsolide/PPEE8.htm] (date de consultation : 12/06/06).

2) Le plan Orsec a été initialement créé par instruction ministérielle du 5 février 1952, mis à jour dans le décret n° 2005-1157 du 13/09/2005 dans le cadre de la loi n° 2004-811.

L'anticipation des situations imprévues doit faire l'objet d'une politique de prévention des risques afin d'assurer la continuité des activités (ou la continuité de services ou la reprise des activités) après un sinistre (ou dans des situations à risques) tels que tremblements de terre, inondations, incendies, attentats, malveillance, pannes majeures, etc.

Historiquement, les organisations ont déjà mis en place des plans d'urgence sur incident (Emergency Response Plan) ou des plans de reprise sur sinistre (Disaster Recovery Plan) qui étaient le plus souvent limités aux ressources informatiques et réseaux.

L'objectif du présent document va au delà en considérant la continuité de l'activité métier de l'entreprise qui est d'assurer la continuité des services critiques rendus à ses clients.

Un PCA pourra couvrir par exemple des aspects touchant à l'environnement même de l'implantation d'un ou de plusieurs sites, à l'organisation dans sa globalité, à un département, aux processus métiers, à une application, en cas d'indisponibilité provisoire ou permanente du service aux utilisateurs.

Dans ce cadre, deux scénarios sont étudiés :

- Indisponibilité d'immeuble (totale ou partielle) ;
- Indisponibilité de l'Informatique et Télécoms (totale ou partielle).

Les scénarios envisageables pour assurer les missions listées ci-dessus sont divers ; ils prennent en compte à la fois les ressources humaines et matérielles (Cf. schéma page 9).

Les PCAs existants adressent souvent en premier lieu une notion de sinistre localisé, par exemple l'incendie d'un site, d'un bâtiment, d'un étage, d'une salle. Ils prévoient des procédures pour que l'organisation puisse fonctionner malgré tout, dans une situation dégradée, et le PCA intervient jusqu'à rétablissement d'une situation normale qui peut différer de celle d'origine avant sinistre. Pour autant, tout en privilégiant la prise en compte des risques endogènes, les études menées dans le cadre du PCA permettront de traiter les risques exogènes (exemple : pandémie, défaillance de prestataire essentiel, catastrophes naturelles, ..). Ces situations ayant une ampleur qui peut dépasser le simple cadre de l'organisation, il conviendra de tenir compte des mesures gouvernementales prévues et d'adapter le PCA en conséquence.

Le présent document a pour objectif de spécifier des bonnes pratiques en matière de Plan de Continuité d'Activité dans des situations à risques, pendant ou après un sinistre.

En revanche, il ne traite pas des discontinuités d'activité non liées, directement ou indirectement, au système d'information comme la pénurie de matières premières (ex : silicium), les défauts de production (ex : malfaçon entraînant une perte d'image), etc.

3 Contexte normatif, réglementaire et autres travaux existants

À ce jour, il n'existait aucune règle normalisée en France permettant de s'assurer et de mesurer l'adéquation entre d'une part les besoins utilisateurs exprimés par une organisation et d'autre part la solution choisie et mise en place après un sinistre, d'où la rédaction du présent référentiel par un groupe Afnor qui a travaillé de décembre 2005 à décembre 2006 pour aboutir à la publication du présent document.

Que ce soit en Europe ou au plan international, il existe cependant de nombreuses réglementations, normes et des travaux en cours qui abordent le sujet de la continuité d'activité.

Nous citerons à titre d'exemples pour le domaine réglementaire, les décisions du comité Bâle II sur le contrôle bancaire international, la loi française n° 2003-706 sur la sécurité financière qui précise des exigences fortes en termes de procédures de contrôle interne, le règlement (France) CRBF 2004-02 qui fait référence à un plan de continuité d'activité documenté, cohérent et testé, et la loi américaine Sarbanes-Oxley qui, même si elle n'exige pas la mise en place d'un PCA, pose des exigences sur les contrôles et procédures appliqués aux systèmes d'information produisant de l'information financière.

Les principaux standards et normes qui abordent le thème de la continuité d'activité -soit partiellement, soit de façon plus détaillée- sont :

- La norme ISO/IEC 17799 *Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour la gestion de la sécurité de l'information* ;
- Le projet ISO/IEC 24762 *Guidelines for information and communications technology disaster recovery services* ;
- Le guide anglais BSI PAS 56 *Guide to Business Continuity Management* (PAS pour Publicly Available Specification) ;
- Le standard international ITIL, Service Delivery, section 7 : *IT Service Continuity Management* ;
- La norme australienne HB 221 — 2004 : *Business Continuity Management* ;
- L'instruction générale 170/98 : *Business Continuity* du *Defence Council* britannique ;
- La norme américaine NFPA 1600 — 2004 : *Standard on Disaster/Emergency Management and Business Continuity Programs*.

Cette liste est non exhaustive, et il existe encore de nombreuses productions normatives et réglementaires en cours de réflexion, révision et/ou de développement de par le monde.

4 Termes et définitions

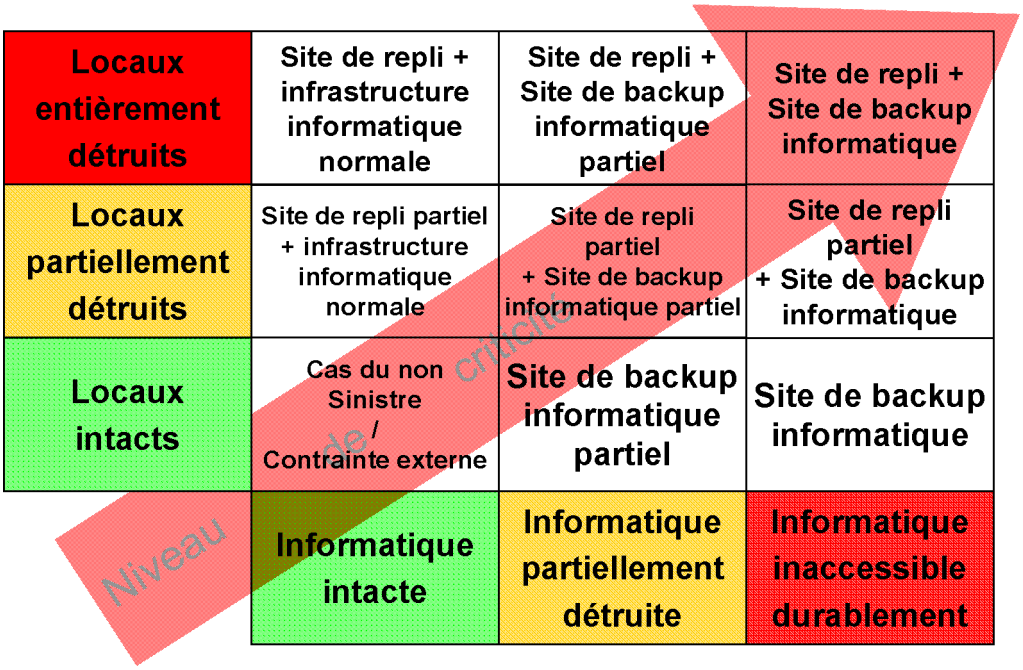
Dans le présent document, le PCA s 'appuie principalement sur le «Plan de Continuité des Opérations» (PCO) et le «Plan de Continuité Informatique et Télécommunications» (PCIT) dont le contenu est précisé dans les pages suivantes.

Un glossaire proposé en **annexe** rassemble la terminologie en rapport avec la continuité d'activité.

5 Schéma : situations à couvrir

Les entreprises et/ou organisations doivent faire face à plusieurs situations de sinistres.

Le schéma ci-après présente quelques-unes d'entre elles sur la base des composantes «locaux» et «informatique» avec leurs différents niveaux de criticité :



Pour être complet ce schéma doit de plus considérer la composante «personnel» pour tenir compte d'une part des risques sociaux (ex : grève totale ou partielle) et des risques liés à une pandémie (le personnel ne se déplace plus).

Des solutions de connexion à distance pour les activités les plus critiques peuvent dans certains cas apporter un élément de solution.

6 Choix stratégiques de mise en place d'un PCA

La mise en place d'un PCA est, en soi, un choix stratégique pour toute organisation. Ce choix consiste à mettre en œuvre une solution de secours opérationnelle face à des scénarii de sinistres identifiés qui peuvent aller de l'indisponibilité d'une machine critique à l'indisponibilité d'un ou de plusieurs bâtiments, en passant par l'indisponibilité du système d'information ; et ce, quelque soit l'origine du sinistre.

Une fois que la mise en place d'un PCA est décidée, les choix stratégiques résident dans les solutions à mettre en place au regard des enjeux et des impacts pour l'organisation.

Le secteur d'activité, la sensibilité face au risque, la culture du risque dans l'organisation, le positionnement de l'organisation, sont autant de critères, non limitatifs, qui vont influencer les choix stratégiques de mise en place d'un PCA et son dimensionnement.

Les choix organisationnels et d'architecture de mise en place d'un PCA découlent d'une analyse d'impact (financier, image de marque, juridique, etc.) relative à un arrêt potentiel, total ou partiel, des services nominaux de l'organisation.

Ces choix sont eux-mêmes porteurs de risques résiduels inhérents aux types de sinistres qui sont parfois contradictoires. Typiquement, face à un sinistre de type pandémie virale, toutes les solutions basées sur un site de repli utilisateurs seraient insuffisantes, les utilisateurs étant invités à minimiser leurs déplacements par les pouvoirs publics.

De même, un sinistre consécutif à une attaque massive de type virus informatique entraînant une indisponibilité du système informatique aura des conséquences différentes selon les choix qui auront été faits pour l'architecture de secours informatique. En effet, autant une architecture de «mirroring synchrone» est efficace pour garantir une reprise d'activité rapide, autant elle est vulnérable à la propagation de virus, les deux sites étant alors contaminés.

Il revient donc aux instances décisionnelles de l'organisation d'arrêter la stratégie pour le PCA en tenant compte de la mesure des impacts et des risques résiduels consécutifs aux choix retenus.

La formalisation de la stratégie de secours requiert un engagement des instances décisionnelles ainsi qu'une délégation pour la maintenance opérationnelle du PCA.

7 Rôles et responsabilités

Mettre en place un PCA implique que des personnes vont jouer des rôles et auront des responsabilités (dans certains cas très fortes) et ce tout au long des étapes de l'élaboration jusqu'au maintien en condition opérationnelle du PCA.

Ces personnes appartiennent soit à l'organisation considérée, soit à des organisations extérieures (autorités compétentes, cabinet de consultants, avocats, juristes, assurances, partenaires, sous-traitants, …).

Parmi les entités fonctionnelles qui vont intervenir, on distingue :

Une fonction de pilotage (direction du projet), en charge :

— de fixer les objectifs et la stratégie du projet ;

— d'en arbitrer les choix budgétaires ;

— d'en arbitrer les choix de planning ;

— d'allouer les ressources de toutes sortes pour la réussite du projet ;

— de vérifier que les objectifs sont atteints.

Une fonction de management décisionnelle, en charge :

— de décider ou non d'activer tout ou partie du PCA (sur les recommandations faites par la fonction de management opérationnelle formalisées dans un dossier de décision) ;

— d'assurer la direction du PCA au plus haut niveau.

Une fonction de management opérationnelle, en charge :

— d'évaluer la situation et de recommander ou non à la fonction de management décisionnelle d'exécuter le PCA ;

— d'assurer la direction opérationnelle du PCA sur le terrain ;

— de coordonner la maintenance en conditions opérationnelles du PCA.

Une fonction de responsable du PCA, en charge :

— de la coordination du redémarrage des activités vitales sur le(s) sites(s) dont il a la charge.

Une fonction de communication, en charge :

— d'élaborer la stratégie de communication interne et externe (presse) en cas d'activation du PCA ;

— d'assurer la communication du retour à la situation nominale.

Tableau de synthèse

	Élaboration	Implémentation	MCO	Cellule de crise	PCA	Retour situation nominale
Pilotage projet	X	X	X			X
Management décisionnel	X			X	X	X
Management opérationnel			X	X	X	X
Responsable PCA				X	X	X
Communication				X	X	X

8 Organisation du PCA

Le PCA est structuré autour de 5 grands thèmes :

1) Remontées d'Incidents, évaluation et alerte ;
2) Gestion et pilotage du PCA : cellule de gestion de crise ;
3) Plan de Continuité des Opérations (PCO) ;
4) Plan de Continuité Informatique et Télécoms (PCIT) ;
5) Maintien en Condition Opérationnelle (MCO).

8.1 Remontée d'incidents, évaluation de la situation et alerte

Il s'agit, suite aux remontées d'incidents :

— d'évaluer la gravité de la situation ;

— de déterminer s'il s'agit d'une crise nécessitant :

- la mise en alerte des membres des cellules ;
- la convocation ou non des cellules de décision et de pilotage ;
- le choix et la mise en oeuvre des actions conservatoires immédiates.

Lors de l'analyse, il s'agira d'évaluer par constat de sinistre ou d'incident majeur, le niveau d'alerte et d'urgence des convocations.

Cette évaluation pourra se faire au travers de grilles prédéfinies.

Suite aux remontées d'incidents, les informations à collecter et à transmettre seront :

- La nature de l'évènement et les conséquences ;
- La durée prévisible de l'interruption ;
- Les mesures prises ou envisagées ;
- Les personnes informées ;
- Les facteurs d'aggravation éventuels ;
- Les coordonnées des partenaires à mettre en alerte, des hébergeurs, fournisseurs, administration.

8.2 L'Organisation de crise

Le PCA définit les missions de la cellule de crise décisionnelle (CCD).

La CCD est chargée principalement d'arbitrer les décisions stratégiques, de gérer les imprévus, de financer l'urgence et de coordonner la politique de communication.

Elle s'appuie pour cela sur :

- la cellule de crise opérationnelle (CCO) ou cellule de coordination qui a pour mission de faire un état des lieux, d'activer, de coordonner et contrôler la bonne exécution des tâches du PCA, de centraliser les informations, d'analyser et traiter les imprévus, de réaliser les synthèses d'avancement et recommandations d'ajustements stratégiques à destination de la «Cellule de Crise Décisionnelle» ;

  Pour réaliser ses missions, la CCO s'appuie sur les équipes de support (logistique, informatique, ressources humaines) et les équipes métiers qui accomplissent les tâches du PCA.

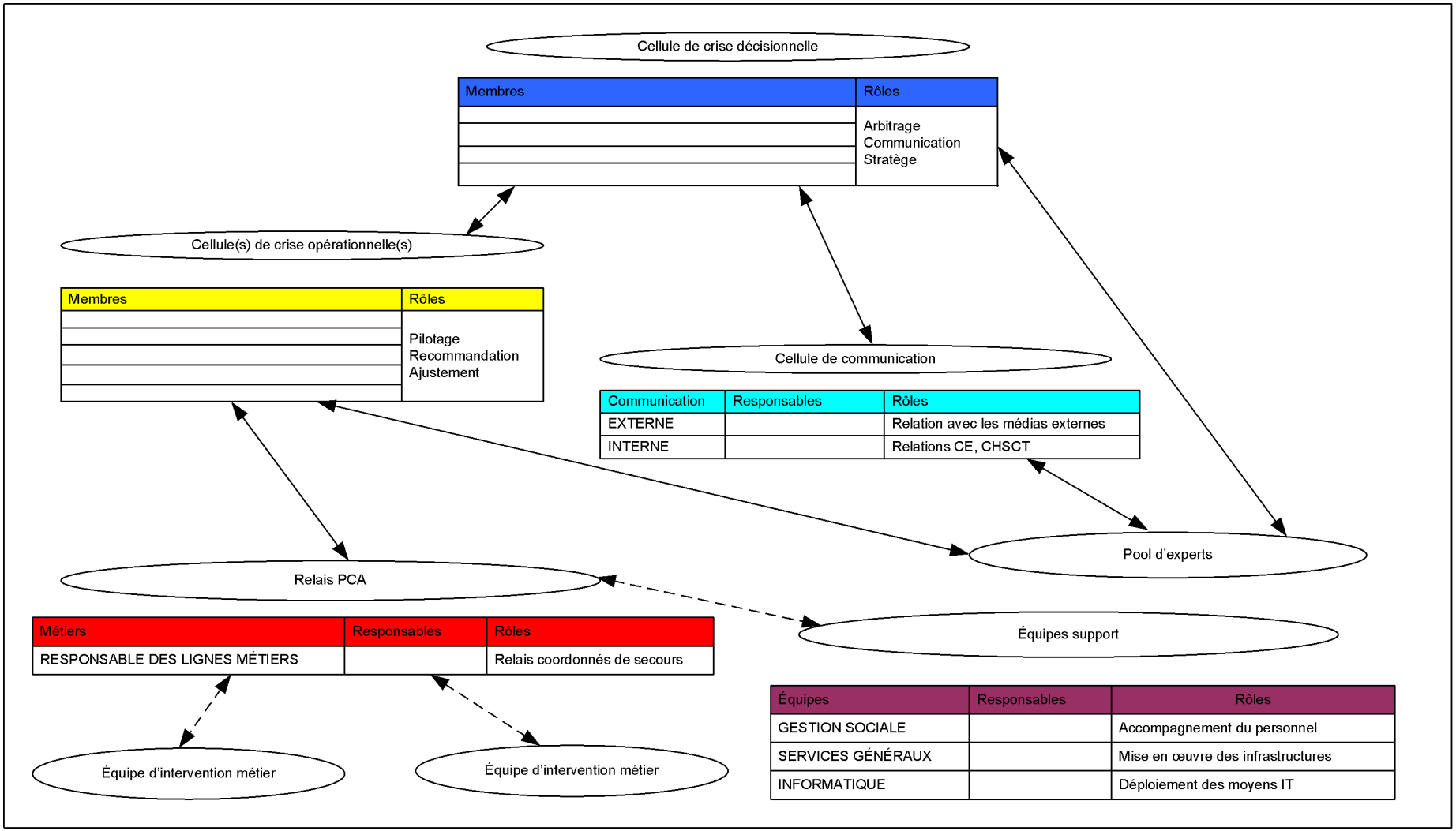
- la cellule de communication qui est en charge de la définition et de la mise en œuvre de la politique globale de communication externe et interne ;
- la cellule d'expertise qui a pour objet d'analyser et de traiter les imprévus et de capitaliser l'expérience ;
- la ou les cellules de crise des autorités (ministère, préfecture, mairie, etc.).

La gestion de crise doit inclure un processus d'escalade qui permet de qualifier la gravité de l'incident et d'adapter en conséquence l'organisation de crise mise en place.

Ce processus d'escalade doit comprendre :

- une définition des **niveaux de gravité** bâtie sur l'impact de l'incident pour l'entreprise, par exemple :
  - **Incident local** : Évènement n'ayant pas d'impact fort sur le déroulement des processus métier de l'entreprise ;
  - **Incident significatif** : Évènement dégradant le déroulement de certains processus métiers et pouvant avoir un impact majeur sur l'entreprise ;
  - **Incident majeur** : Évènement dégradant fortement le déroulement des processus métiers et ayant un impact sur la pérennité de l'entreprise ;
- L'identification des **acteurs validant chaque niveau de qualification,** par exemple :
  - **Incident local** : Évènement qualifié par la structure informatique avec selon le niveau de gravité technique alerte du management de la structure informatique ;
  - **Incident significatif** : Évènement qualifié par le management de la structure informatique de l'entreprise avec alerte de la direction de l'entreprise ;
  - **Incident majeur** : Évènement qualifié par la direction de l'entreprise ;
  - **L'organisation de gestion de crise** mise en place**,** par exemple :
    - **Incident local** : Cellule de crise de la structure informatique ;
    - **Incident significatif** : Cellule de crise de la structure informatique en liaison avec la ou les cellules de crise des métiers concernés ;
    - **Incident majeur** : Mobilisation de l'ensemble du dispositif de crise sous pilotage de la cellule de crise de la direction de l'entreprise.

Schéma d'organisation de crise



8.3 Le Plan de Continuité des Opérations (PCO)

Le Plan de Continuité des Opérations couvre la perte des locaux des utilisateurs conduisant au repli des utilisateurs sur un autre site.

Ce site de repli utilisateurs doit notamment prendre en compte :

- le nombre de positions de travail dès la reprise ainsi que pour la montée en charge ;
- les procédures fonctionnelles de reprise des activités ;
- la présence sur le site de repli utilisateurs de dossiers et documents liés au système d'information ;
- la présence sur le site de repli utilisateurs de dossiers et documents non informatiques ;
- la perte du Système d'Information (SI) nécessaire aux processus métier des utilisateurs impliquant la mise en place de mesures de contournement pour assurer le bon déroulement des processus métier en attentant le redémarrage du SI. Ces mesures s'appuient sur des mesures conservatoires, moyens préalables mis en place afin de pouvoir contourner un sinistre (extractions de données vers les outils bureautiques, préparation d'états papier, etc.).

8.4 Le Plan de Continuité Informatique et Télécoms (PCIT)

Un PCIT nécessite la définition, la préparation, les tests, les exercices, la maintenance et, le cas échéant, la mise en œuvre de ce pour quoi il a été conçu : pallier la perte d'un site après un sinistre et décision de la cellule de gestion de crise d'activer le plan de reprise d'activité. Il représente donc l'ensemble des moyens techniques informatiques et télécoms, bâtiments, et ressources techniques nécessaires à la réactivation de l'infrastructure Informatique et Télécoms sur le site de secours tel que défini dans le plan.

Chacun des moyens techniques inclus dans ce périmètre nécessite une mise en œuvre qui lui est propre, en fonction du contexte technique dans lequel il s'insère pour réaliser une fonction particulière qui n'est pas forcément identique au site original (mode dégradé). Par ailleurs, ces moyens techniques font appel à des compétences variées et à plusieurs intervenants, chacun dans son domaine d'expertise. Dans un contexte de crise et d'activation du PCIT, la pression pour tenir les engagements sur les temps de redémarrage est énorme et, souvent, toutes les personnes compétentes ne sont pas disponibles.

Il convient donc de se prémunir contre ce risque majeur en mettant en place des procédures pour la mise en place, le suivi et les recettes de chaque composant du PCIT qui doivent, théoriquement, pouvoir être appliquées par une personne disposant d'un niveau minimum de connaissances sur le domaine traité.

Ces procédures traitent de toutes les phases de mise en œuvre de chaque composant :

- Conditions de déclenchement de la procédure, délai maximum de mise en œuvre, contacts pour support.
- Contact pour «reporting» sur l'avancement et l'escalade en cas de souci, localisation des ressources nécessaires (documents, matériels, fournisseurs, …).
- Etat des lieux des ressources nécessaires et inventaire préalable.
- Synchronisation avec d'autres composants ou ressources.
- Installation des équipements et recette.
- Configuration des équipements et recette.
- Tests de bon fonctionnement et recette.
- Clôture de la tâche et «reporting».
- Maintien à disposition si nécessaire : durée, conditions du maintien, levée et passage éventuel en astreinte et conditions.

Chacune des phases comporte tous les éléments nécessaires à une mise en œuvre par une personne disposant des compétences minimum et n'étant pas forcément spécialiste du domaine concerné (ex : sous-traitant). La documentation est un élément fondamental car elle ne fait apparaître que l'essentiel, ce qui est directement utile dans un contexte d'urgence et de pression forte, tout en laissant la possibilité de contacter un expert le cas échéant (ex : assistance 24 × 7 chez le fournisseur ou le prestataire). Elle est claire, concise, ne prête pas à interprétation et donne des objectifs mesurables à court terme afin de détecter au plus tôt une dérive (retard) dans la mise en œuvre pour reporting de l'avancement unitaire et global.

Ces procédures étant très directives et réduites à l'essentiel, elles sont rejouées régulièrement afin d'en conserver la qualité et l'efficacité dans le cadre soit de vérifications unitaires, d'exercices limités ou grandeur nature (voir § MCO).

L'organisation de ces procédures est calquée sur le mode projet avec des niveaux de détail correspondant au rôle de chacun (macro pour le responsable du PCIT, de plus en plus précis jusqu'au composant unitaire), des responsables identifiés, des ressources, des charges et délais, des points de synchronisation et des dépendances.

Ces procédures ainsi que tous les outils afférents (projet, documentations, contacts, …) sont mis à disposition sur des supports inaltérables (ex : papier plastifié), ne nécessitant pas de moyens techniques sophistiqués pour leur utilisation (ex : stylo), et dupliqués sur des localisations géographiques adéquates. Elles font l'objet d'audits réguliers indépendants afin de s'assurer de leur qualité et pertinence.

8.5 Le Maintien en Condition Opérationnelle (MCO)

Comme nous l'avons vu précédemment, les PCO et PCIT s'appuient essentiellement sur l'exécution de procédures, soit métier, soit techniques. Ces procédures reposent sur un ensemble de compétences, de technologies, d'intégrations et de mises en œuvre qui évoluent en permanence dans le temps, soit par nécessité pour adapter les outils aux besoins des métiers, soit par obligation suite à l'évolution nécessaire des technologies. Il appartient donc aux responsables des PCO et PCIT de s'assurer que les procédures demeurent opérationnelles d'un point de vue technique et pertinentes d'un point de vue métier.

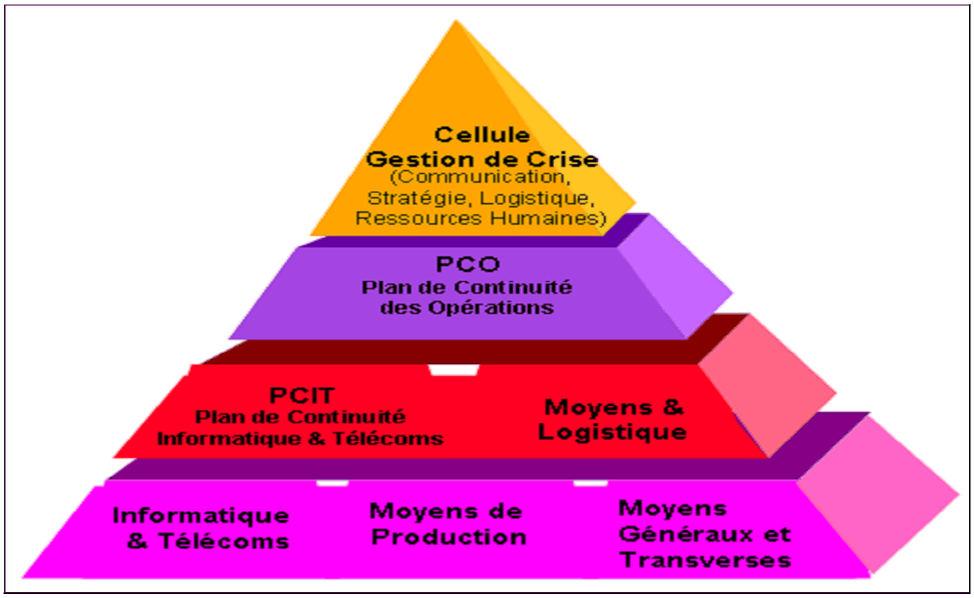
Le MCO touche donc autant l'Informatique et Télécoms que les métiers qui font évoluer leurs modes opératoires parallèlement à l'évolution de leur métier et des contraintes auxquelles ils sont soumis. Par exemple, si la paie fait partie des fonctions vitales, il est nécessaire de maintenir à jour la documentation des procédures internes et externes correspondantes afin qu'elles soient toujours utilisables et applicables selon le périmètre assigné et avec les outils disponibles en mode normal et en mode dégradé. Négliger ce point peut, dans certains contextes délicats, aboutir à une grève bien plus préjudiciable qu'un sinistre.

De son côté, l'Informatique et Télécoms intègre, dès la conception, des infrastructures, des applications, de la production ainsi que les mécanismes permettant d'identifier les relations entre composants afin de maîtriser la chaîne des contraintes. Il est alors possible d'identifier les composants impactés, à quel niveau (neutre, fonctionnel, configuration, technique, ressources, …), et d'intégrer dans les budgets prévisionnels les coûts associés au maintien en conditions opérationnelles. Cela se traduit par la «gestion du changement» qui est ainsi formalisée ou mise en valeur et qui fait partie intégrante du cycle de vie du PCIT.

Tout ce qui en découle est ensuite question d'organisation, de moyens et d'outils selon les choix et contraintes propres à chaque organisation.

9 Schéma des procédures de mise en œuvre

Le schéma suivant présente les éléments essentiels sur lesquels s'appuie un PCA :



Ce schéma présente une pyramide à quatre niveaux :

- Niveau 1 : c'est la base de la pyramide, il traite des moyens permettant d'assurer les services.
- Niveau 2 : il traite du plan de continuité concernant l'Informatique et Télécoms ainsi que des moyens et de la logistique.
- Niveau 3 : c'est le plan de continuité opérationnelle qui a en charge d'assurer la continuité des opérations et autres actions de l'activité.
- Niveau 4 : il concerne la cellule de gestion de crise qui est le centre nerveux du PCA.

9.1 Niveau 1 : moyens de production Informatiques et Télécoms/moyens généraux et transverses

Il est nécessaire de mettre en œuvre un ensemble d'actions permettant de réduire les risques de pannes, d'incidents, d'indisponibilité afin de limiter en cas de sinistre, l'ampleur des conséquences qui pourraient en découler (impacts). Pour cela, les différents éléments qui participent au cœur des activités de l'organisation sont concernés : l'Informatique et Télécoms, les moyens et matériels de production ainsi que les moyens généraux et transverses.

Ces moyens doivent être régulièrement analysés afin d'en réduire les faiblesses, notamment :

- structure des moyens informatiques et télécoms ainsi que les solutions de back up (interne ou externe) ;
- contrôles d'accès physique et sécurité physique concernant le(s) site(s) de production ;
- structure et fourniture d'énergie notamment en situation de crise ;
- protection face aux risques majeurs (incendie, dégâts des eaux, …) ;
- climatisation ;
- relations et coordination avec l'ensemble des moyens transverses, les clients, l'ensemble des partenaires et contreparties ainsi qu'avec les sous-traitants ;
- matériels de production et autres moyens.

Après mise en évidence des points faibles, des mesures adaptées sont mises en œuvre dans des délais et des coûts compatibles avec les objectifs.

9.2 Niveau 2 : PCIT/Moyens et Logistique

Le PCIT ne traite que des aspects liés aux infrastructures informatiques et télécoms ainsi que des moyens généraux et transverses nécessaires à l'exécution d'un plan de continuité.

Le PCIT permet un redémarrage des environnements techniques et applicatifs en traitant notamment des points suivants :

- choix du site et emplacement géographique du site de secours (interne ou externe) ;
- contrôles d'accès physique et sécurité physique sur ce site ;
- fourniture de puissance électrique ;
- climatisation ;
- administration des chemins et câblages ;
- ensemble des matériels informatiques et télécoms de secours ;
- relations et coordination avec les moyens transverses, les clients, l'ensemble des partenaires et contreparties ainsi qu'avec les sous-traitants.

9.3 Niveau 3 : le Plan de Continuité des Opérations (PCO)

Le Plan de Continuité des Opérations (PCO) prend en compte l'angle «procédures Métiers» de l'entreprise ce qui sous entend :

— les procédures et outils de fonctionnement en mode dégradé, de contournement ou de substitution ;

— dans certain cas, la mise à disposition d'un site de repli utilisateurs (structure de repli pour les métiers) incluant les locaux de repli avec les infrastructures (machines, lignes de production, entrepôts,...), les matériels (bureaux, chaises, positions, téléphone etc.), les éléments du système d'information non informatique ainsi que toutes les procédures métiers attachées.

Le site de repli utilisateurs doit notamment prendre en compte :

- le nombre de positions de travail dès la reprise ainsi que pour la montée en charge ;
- les procédures fonctionnelles de reprise des activités ;
- Les éléments du système d'information nécessaires et qui ont été remis en activité, le cas échéant (voir PCIT) ;
- la présence sur le site de repli utilisateurs de dossiers et documents liés au système d'information ;
- la présence sur le site de repli utilisateurs de dossiers et documents non informatiques ;
- si besoin des matériels de production non informatiques.

Le PCO traite des problématiques d'organisation, de planification et de moyens. Le PCO est un outil qui permet de réagir à un événement imprévu et selon des scénarios prédéfinis afin de maintenir le cœur de l'activité de l'organisation. Il vise à enchaîner un ensemble de tâches et moyens prédéfinis, dans des délais déterminés à l'avance.

9.4 Niveau 4 : la cellule de gestion de crise

Cette cellule est composée des personnes qui ont la charge de prendre les décisions concernant la continuité des activités :

- analyse de la situation en lien avec les responsables opérationnels (autorités, pompiers, Risk manager, …) ;
- décision ou non d'activer le plan de continuité et de déclarer le retour à la situation nominale ;
- tenue de la main courante et élaboration du bilan de crise ;
- gestion du scénario de continuité à appliquer ;
- gestion de la communication interne et externe ;
- gestion et coordination des ressources humaines ;
- vérification de la continuité de services, y compris celle des sous-traitants.

Cette cellule est en général complétée par des conseillers techniques afin d'avoir une vision la plus juste possible de la situation (ex : responsables RH, DSI, RSSI, juristes, assurances).

10 Démarche d'un PCA

Comme il est précisé au début de ce document, son objectif est de spécifier les bonnes pratiques en matière de PCA dans des situations à risques, pendant ou après un sinistre.

Nous venons de préciser les différents composants d'un PCA, l'objectif de ce paragraphe est maintenant de proposer une démarche à destination du responsable du projet PCA, pour l'aider à définir, mettre en œuvre et rendre opérationnel un PCA.

10.1 Présentation de la démarche

Pour mener à bien ce projet PCA, il est important, comme dans tout projet de le décomposer en phases :

— Phase 1 — Élaboration du PCA ;

— Phase 2 — Implémentation du PCA ;

— Phase 3 — Maintien en Condition Opérationnelle ;

Chaque phase répond à un ou plusieurs objectifs et sa réalisation se décompose en étapes.

D'autre part, les phases 2 et 3 (implémentation et MCO) seront elles-mêmes découpées suivant qu'il s'agit de PCO, de PCIT ou de cellule de crise.

Enfin, une phase ne peut être lancée que si la précédente a été réalisée.

10.2 Schéma de la démarche

Comme on vient de le voir, un PCA présente dans sa démarche 3 phases distinctes :

- la première phase consiste à élaborer le PCA afin d'identifier les moyens de son support ;
- la deuxième phase durant laquelle l'implémentation du PCA est assurée jusqu'à ce que le PCA soit opérationnel ;
- enfin la troisième phase, dont l'objectif consiste à assurer le maintien en condition opérationnelle du PCA déployé.

Voici à travers les trois tableaux qui suivent, le détail de ces différentes phases :

10.3 Phase 1 : Élaboration du PCA

Phase 1 — Élaboration du PCA
Objectif — Identifier les besoins de continuité : Processus métiers et fonctions critiques Délai d'Interruption Maximum Admissible (DIMA) Perte de Données Maximum Admissible (PDMA) Ressources humaines et matérielles ↳ Étape 1 — Cadrage et définition du Projet ↳ Étape 2 — Identification des processus métiers critiques : analyse d'impact
Objectif — Définir les solutions pour assurer la continuité des métiers et des fonctions critiques
↳ Étape 3 — Définition du scénario du PCA ↳ Étape 4 — Définition des moyens du PCA : choix de la stratégie et des moyens
◆ Les moyens de support du PCA sont définis

10.4 Phase 2 : Implémentation du PCA

Phase 2 — Implémentation du PCA		
Plan de Continuité des Opérations (PCO)		**Plan de Continuité Informatique et Télécoms (PCIT)**
Objectif **— Élaborer et mettre en place la logistique de continuité et de reprise fonctionnelle**		Objectif **— Élaborer et mettre en place l'architecture de continuité**
Étape 5 — Validation par des tests unitaires de l'architecture des moyens de continuité — fusionner étapes 5 et 6		
Étape 6 — Procédures de maintien des moyens de continuité rédigées		
Objectif **— Élaborer les procédures de continuité et de reprise des métiers et des fonctions ritiques**		Objectif **— Élaborer les procédures techniques de continuité et reprise echnique et fonctionnelle**
Résultat — Procédures rédigées et validées		
Cellule de gestion de crise (communication, stratégie, logistique, ressources humaines)		
Étape 7 — Élaboration et mise en place des procédures de la cellule de crise		
Objectif — **Organiser la communication (interne, externe)**		
Résultats — Procédures rédigées et validées — Cellule structurée		
Objectif **— Former et tester**		Objectif **— Former et tester**
Étape 8 — Formation des équipes		
Étape 9 — Test pour validation du PCIT		
Étape 10 — Test pour validation du PCO		
Étape 11 — Test pour validation de la gestion de crise		
Remarque : En fonction de la structure de l'organisation, les étapes 9 à 11 peuvent être menées indépendamment les unes des autres et/ou globalement.		
◆ Le PCA est opérationnel		

10.5 Phase 3 : Maintien en Condition Opérationnelle (MCO)

Phase 3 — Maintien en Condition Opérationnelle (MCO)		
Maintenance du PCO	Maintenance cellule de crise	Maintenance du PCIT
Objectif **— S'assurer du caractère opérationnel des plans**		
↳ Étape 12 — Mise à jour des plans ↲		
↳ Étape 13 — Tests des plans ↲		
◆ Le PCA est maintenu opérationnel		

11 Formation et tests

11.1 Formation

Le PCA est en phase finale d'implémentation : les moyens en sont identifiés et connus. Certains existent déjà, d'autres sont réservés, ou bien seront approvisionnés seulement en cas d'activation du PCA. Les procédures correspondantes ont été rédigées. C'est donc le moment de former les acteurs au PCA, afin que l'ensemble de l'organisation mise en place soit connue, et que les procédures soient maîtrisées.

Pour mener à bien cette formation, il conviendra de :

- Rédiger le plan de formation au PCA (dont les supports de formation) ;
- Gérer et animer les sessions de formation conformément au planning prévu ;
- Créer un formulaire permettant d'établir le bilan qualitatif et quantitatif de la formation.

Le plan de formation comprendra :

1) La définition de sa cible :
   - Toute l'entreprise, pour information générale (exemple : technique de e-learning sous intranet) ;
   - Les acteurs du PCA, en tant qu'opérationnels PCA, au cours de session de formation ad hoc ;
2) Les supports de formation adaptés à chaque cible ;
3) Le calendrier des formations ;
4) La définition du suivi qualité et du reporting des formations.

11.2 Tests

Lorsque les acteurs auront été formés, il sera alors possible de tester le PCA. Les tests sont le seul moyen de vérifier que l'ensemble du dispositif fonctionne. C'est donc une étape très importante pour s'assurer que le PCA est effectivement opérationnel.

Un PCA qui n'a pas été testé ne peut pas être considéré comme un PCA opérationnel, et par conséquent il subsiste des risques résiduels.

On identifie :

- Des tests unitaires : pour tester séparément les procédures les plus critiques du PCA ;
- Un test global de bout en bout, appelé test de filage, pour vérifier la cohérence de l'ensemble.

Pour mener à bien l'étape des tests, il conviendra dans un premier temps de rédiger le plan de test du PCA (dont support), ensuite, lors de la phase de conduction des tests pouvant être menée sur la base d'un certain nombre de journées de test (à définir) de conduire les tests du PCA. Enfin, pour chacun de ces deux tests, il faudra prendre en compte les corrections en résultant.

Note importante sur la documentation

Que ce soit pour la formation comme pour les tests, il conviendra de rédiger un certain nombre de documents, avant, pendant et après ces deux étapes. On devra réaliser parmi les livrables : le plan à jour et ses supports de formation ainsi que la documentation revue et corrigée liée aux tests.

12 Retour à la situation nominale

La cellule de gestion de crise a activé le PCA et en pilote l'exécution jusqu'au retour des opérations à une situation préalablement définie comme «normalisée», c'est-à-dire correspondant à un état stabilisé où chacun des services importants de l'organisation a retrouvé un mode de fonctionnement jugé satisfaisant.

Cette situation «normalisée» ne correspond pas à l'état «avant le sinistre» puisque, par définition, il y a eu une atteinte majeure aux capacités opérationnelles de l'organisation, d'où le déclenchement du PCA.

Par ailleurs, le PCA a pour objectif de ne restituer que le minimum de capacités opérationnelles permettant à l'organisation d'exécuter ses fonctions vitales puis, selon un planning de montée en charge, arriver à une situation stabilisée ou «normalisée» telle que décrite précédemment.

À ce stade, les prestations de services techniques et logistiques de secours peuvent être stoppées. Sur ce point, il est important de noter que seule la fonction de pilotage est habilitée à décider ou non du retour à une situation jugée «normale».

Généralement, deux situations sont retenues dans le cadre de sinistres :

1) le retour à la normale permettant de revenir à une situation identique à celle avant le sinistre : les dommages subis sont temporaires et limités ;
2) le retour à la normale nécessitant des travaux importants et une relocalisation permanente : les dommages subis sont irréversibles.

Dans ce dernier cas, on parlera plutôt de «situation antérieure» afin de mettre en avant qu'il s'agit essentiellement de restaurer les mêmes niveaux de capacités opérationnelles de l'organisation impactée. Ces capacités ne seront pas forcément restaurées à l'identique, notamment du fait de l'évolution des technologies et de l'obsolescence des matériels qui imposeront l'approvisionnement de configurations différentes. Enfin, on peut s'attendre à un impact sur les modes d'organisation, car un événement d'une telle ampleur est souvent l'occasion d'évolutions à différents niveaux.

Bien que la reconstruction de l'outil de travail de l'organisation ne fasse pas partie intégrante du PCA, le lecteur trouvera ci-après quelques axes de réflexions :

- **RH** : comment maintenir le personnel longtemps dans les conditions de travail particulières (positions de secours), comment anticiper sur les frais supplémentaires occasionnés sur le long terme, la restauration du personnel, les temps de trajet et le découragement qui pourrait s'en suivre avec la perte potentielle de collaborateurs, …
- **Logistique** : comment traiter tous les aspects liés à la reconstruction de nouveaux bâtiments, les besoins sont-ils connus, les délais et procédures administratives maîtrisés, les compétences identifiées et réservées, les problèmes d'adresses postale et de livraison, …
- **Technique** : comment anticiper sur la nécessaire migration vers des plateformes plus récentes et les impacts qui en découlent, les délais de commande et livraison des fournisseurs, les coûts supplémentaires associés, …
- **Métiers** : comment résorber dans le temps les retards accumulés lors de la crise, notamment avec des moyens forcément réduits tant que le retour à la situation nominale n'est pas achevé, a-t-on prévu les modes opératoires et procédures avec nos fournisseurs et clients dans cette phase, le rattrapage des situations qui ont fini devant les tribunaux, …

Un bilan global du retour à la situation nominale devra être réalisé.

Pour ce faire, il appartiendra à la fonction de pilotage de réclamer un compte rendu auprès de chacune des fonctions impactées par l'activation du PCA comme de son déroulement.

Une fois ces rapports récoltés, la fonction de pilotage pourra formaliser une synthèse de retour à la situation nominale : il s'agira du bilan global.

Les objectifs de ce bilan global pourront alors faire apparaître les besoins en matière de :

- corrections/modifications des éventuels dysfonctionnements constatés aux regards des actions prises lors du déclenchement comme du déroulement du PCA ;
- identifications des impacts et adaptations des éventuelles prestations/solutions nécessaires suite au déroulement du PCA et dont celui-ci reste tributaire.

13 Le facteur humain en situation de crise

13.1 L'élément humain : Un aspect majeur du PCA

Il est essentiel de bien prendre en compte que, lors de la conception du PCA et plus encore lorsque celui-ci devra être mis en œuvre, ce sont des personnes qui agiront pour permettre de continuer les activités dans les meilleures conditions possibles. Il faudra entre autre faire attention au choix des personnes qui composeront les différentes cellules de gestion de crise ; leurs niveaux de responsabilité et implication dans le PCA peuvent impacter le bon déroulement de celui-ci. Savoir prendre les bonnes décisions dans une situation déstabilisée, savoir comment communiquer, avoir prévu la destination des personnes lors de la survenance d'un sinistre sont des actions primordiales au bon pilotage du PCA.

Une attention particulière devra être portée également dans la composition des équipes de chaque cellule de crise qui, le jour J, devront intervenir. (Cf. § 8.2 Organisation de crise).

13.2 Prise en compte de l'impact psychologique

Quelles que soient les circonstances de survenance du sinistre, celui-ci aura un impact plus ou moins fort sur les personnes (management, personnel opérationnel, sous-traitants, clients, etc.). Dans le pire des cas, des personnes peuvent être touchées physiquement (AZF, 11 septembre, tempêtes, incendies, etc.) ou par les conséquences du traumatisme psychologique, mais même dans des situations sans atteinte à l'intégrité des personnes, la désorganisation due à une situation exceptionnelle, voire simplement inhabituelle, peut entraîner une déstabilisation conduisant à une incapacité à réagir.

Il a été démontré que la perte de repère en situation de sinistre affecte fortement la capacité à prendre des décisions y compris celle du management. Cette dimension doit être prise en compte lors de la préparation du PCA. A titre d'exemple extrême, une étude de *globalcontinuity.com* réalisée quelques jours après les événements du 11 septembre 2001 a montré que seules 49% des sociétés directement impactées ont eu le réflexe de déclencher leur PCA et que dans de nombreux cas les bonnes décisions, pourtant prévues dans ce PCA, n'ont pas été prises par le management.

On pourra éventuellement faire appel à des organisations ou cabinets spécialisés dans la prise en charge de l'aspect psychologique. Une cellule de crise psychologique pourrait éventuellement aider lors d'un sinistre majeur au bon déroulement de la mise en place du PCA.

13.3 Forces et faiblesses du PCA

La réussite du pilotage du PCA repose donc en grande partie sur la capacité des personnes à réagir dans les meilleures conditions possibles. Pour cela la préparation du PCA, sa répétition par les actions de tests et sa maintenance en condition opérationnelle sont des actions déterminantes.

Le quotidien professionnel des personnes repose sur tout un ensemble d'actions et de ressources qui doivent être identifiées lors de la préparation du PCA et la rédaction des procédures de continuité. La routine et le savoir-faire des personnes les conduisent souvent à occulter des éléments qui pourraient se révéler critiques en situation de sinistre. Les exemples classiques du chargeur de portable, du carnet d'adresse ou autre mode d'emploi oubliés dans un bureau sinistré sont des détails qui pourront perturber la bonne reprise d'activité d'une procédure pourtant correctement rédigée. La sensibilisation des acteurs et leur mise en condition de PCA sont donc des points importants à prendre en compte.

13.4 Traitement de la RH en cas de déclenchement

Que deviennent les personnes lors du déclenchement du PCA ? Cette réponse est évidemment conditionnée par le type de sinistre et par la stratégie de continuité décidée par l'organisation. Si les bureaux des personnels sont intacts ceux-ci peuvent rejoindre leur poste de travail même si les ressources informatiques ne sont pas immédiatement disponibles.

En cas de destruction totale ou partielle des locaux, une action de communication immédiate doit être faite vers les personnels afin de leur indiquer leur destination (site de repli utilisateurs, retour temporaire au domicile, travail à distance, chômage technique, etc.). Ceci doit être pris en compte par les acteurs des Ressources Humaines (RH) comme une action prioritaire suite à sinistre en raison des responsabilités de l'entreprise liées à la sécurité des personnes sur leur lieu de travail.

Dans les premières heures suivant la survenance du sinistre la cellule de gestion de crise est mobilisée puis les personnes sont contactées en fonction du scénario de reprise prévu. Les démarches administratives pour une mise en chômage technique de tout ou partie du personnel doivent également être prévues par la RH si la situation l'impose.

En cas de relocalisation des personnes sur un site de repli utilisateurs, la RH peut jouer un rôle important dans la logistique.

Le cas échéant, une mise à jour du règlement intérieur peut être nécessaire afin d'une part d'informer les personnels des conditions de travail en cas de sinistre et d'autre part de les sensibiliser sur leur vigilance pour assurer le maintien en condition opérationnelle du PCA.

13.5 Actions de la DG et de la DRH

Le personnel en cas de sinistre

Il y a lieu de distinguer si le sinistre survient pendant ou hors heures ouvrées.

Dans le cas des heures ouvrées, il faut se rattacher à la réglementation et aux procédures d'évacuation définies. Il convient dans ce cadre de s'appuyer sur les «équipiers d'étage» :

- Évacuation ;
- Rassemblement à un point de ralliement ;
- Comptage des salariés.

Dans le cas des heures non ouvrées, il s'agit de pouvoir communiquer avec le personnel de l'entité.

Plusieurs solutions, fonctions de la taille de l'entité, peuvent être envisagées :

- Arbre d'appels téléphoniques :

  Partant de la cellule de pilotage vers les secrétaires des départements et services de l'organisation, celles-ci répercutent l'appel vers leurs collègues respectifs. Ceci nécessite de maintenir à jour une liste fiable de numéros de téléphone du personnel et de rendre celle-ci disponible hors du site sinistré.

- Envoi de messages vocaux, SMS :

  Dans le cadre des procédures de gestion de crise, la décision d'avertir toute ou partie des salariés de l'entité prendra la forme d'une communication sur les téléphones fixes et/ou portables des salariés. La liste des n° devra être à jour et accessible. Il en sera de même de l'outil permettant la diffusion.

- Appel à un Serveur Vocal Interactif :

  Les messages établis suite au sinistre sont présents sur le serveur. Il appartient à chaque salarié d'appeler ce serveur afin de prendre connaissance des informations voire des consignes à appliquer.

  Le n° de téléphone pourra être connu à l'avance des salariés (n° indiqué au dos des badges salariés, sur les cartes de gestion de crise avec les lieux de repli, les contacts, autres n° de téléphones utiles,…) ou être communiqué par une structure d'accueil devant l'immeuble ou le périmètre sinistré.

Il conviendra également de prévoir lors de la mise en place du PCA, les équipes de sécurité internes à l'entreprise (CHSCT — Comité d'hygiène, de sécurité et des conditions de travail).

Information vers des parents proches

En cas de sinistre ayant entraîné des conséquences physiques sur les personnes, des dispositions doivent être prises pour contacter les parents proches. Ces informations doivent être disponibles, à jour et accessibles hors du site. Un représentant du management de la cellule de pilotage du PCA doit être désigné et formé pour une communication de telle nature.

Support financier

Un sinistre peut avoir des implications financières directes pour les employés [3)]. Le scénario de continuité peut inclure le travail à distance depuis le domicile de l'employé. Dans ce cas des dispositions financières peuvent prévoir la prise en charge des frais de communication voire l'achat d'un poste de travail pour permettre à l'employé d'assurer tout ou partie de son activité. La prise en charge des éventuels frais de déplacement inhérents au travail sur un site de secours doit être prévue.

3) Les dispositions financières liées aux accidents ou décès sur le lieu de travail ne sont pas abordées ici.

Salaires

Le virement de la paie doit rester fonctionnel pendant la période de sinistre.

Logistique

La sauvegarde externe d'éléments essentiels à la reprise d'activité doit être assurée soit sur un autre site de l'organisation, soit chez un partenaire, soit dans un coffre de banque. De tels éléments peuvent être par exemple des clés cryptographiques racines nécessaires à la reconstitution des dispositifs de sécurité sur un site de repli.

Typiquement la procédure de pilotage du PCA doit être disponible à l'extérieur du site facilement accessible aux membres de la cellule de pilotage. Des dispositions doivent être incluses dans cette procédure pour permettre la mise à disposition en temps voulu de tout élément nécessaire à la cellule de pilotage du PCA (ex : qui va chercher quoi et où).

Financement du PCA et assurances

La mise en place du PCA comme son financement doivent être correctement planifiés en relation avec la couverture assurantielle (cf. § 14 aspects juridiques).

Moyens généraux

La Direction Administrative et Financière (DAF) doit intégrer les problématiques liées au re-routage du courrier et des appels téléphoniques. Des dispositions doivent être prises auprès de La Poste et du fournisseur de ressources téléphoniques pour anticiper les actions nécessaires permettant de demander le re-routage du courrier vers une adresse de repli et le re-routage total ou partiel des appels téléphoniques vers un numéro ou un central téléphonique de secours, voire vers un répondeur téléphonique informant les appelants de la situation en cours.

Secours solidaire

Dans certaines organisations il est possible d'envisager une solidarité de place. Celle-ci peut permettre à l'organisation de gérer l'urgence des premières heures/jours du sinistre en offrant un local et des moyens généraux pour la cellule de pilotage du PCA. Il est souhaitable d'anticiper cette possibilité par des accords préalables et au minimum par la signature d'un engagement du meilleur effort possible en cas de crise.

14 Les aspects juridiques

14.1 Ressources humaines

14.1.1 Avant la crise

Un certain nombre d'actions préventives doivent être conduites avant l'occurrence d'une situation de crise :

Déclaration CNIL :

Lors de la crise, un certain nombre d'informations personnelles relatives aux salariés et, le cas échéant, aux personnels extérieurs travaillant habituellement dans l'entreprise (stagiaires, personnels en «régie») sont utilisées pour la finalité spécifique de traitement de la crise : coordonnées téléphoniques et adresses Internet personnelles, coordonnées des parents proches, moyens de transport habituels, établissement d'un fichier des personnes «clés», etc. Afin de se mettre en conformité avec la Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés, (et sauf dans les entreprises dans lesquelles un correspondant à la protection des données personnelles a été nommé), il faut préalablement déclarer à la CNIL, par le biais d'une simple déclaration modificative, les données personnelles recueillies spécifiquement aux fins de gestion de la crise.

Audit et adaptation des contrats de travail ou des accords collectifs :

La crise peut imposer des mesures d'exception, telles la délocalisation géographique ou l'aménagement des horaires, qui sont parfois en contrariété avec les contrats de travail des salariés ou les accords collectifs. Il est souhaitable d'introduire, par avenant dans les contrats de travail (ou par la renégociation d'un accord collectif), les principales dispositions qui seraient susceptibles d'être prises par l'employeur en cas de crise. Ces dispositions dépendent du secteur d'activité et du type de fonction des salariés : délocalisation du lieu de travail, possibilité de travail à distance, aménagement des horaires, etc.

Adaptation du Règlement Intérieur (RI) :

Le règlement intérieur est un document disciplinaire qui s'impose à tous les salariés de l'entreprise. Il couvre des matières qui sont énumérées spécifiquement par l'article L122-34 du Code du travail, notamment en matière de sécurité et de santé. Contrairement au contrat de travail, c'est un document discuté collectivement qui doit recueillir avant son introduction l'avis du comité d'entreprise, à défaut des délégués du personnel, et le cas échéant du CHSCT. Il est souhaitable d'introduire dans le règlement intérieur certaines des mesures, notamment liées à la sécurité, qui seront prises en cas de crise, voire le cas échéant d'annexer le Plan de Continuité d'Activité au règlement intérieur.

Le recours aux astreintes :

Les conditions de recours aux astreintes sont réglementées par le droit du travail. Il est souhaitable de prévoir par avance l'organisation des astreintes et les personnes concernées en cas de crise.

Anticipation des conséquences financières de la crise pour les salariés :

La perte de salaire imputable à une fermeture temporaire de l'établissement ou à une réduction du temps de travail est partiellement compensée par une allocation spécifique prévue par la loi (article L351-25 du Code du Travail). Dans certains secteurs d'activité, tels le bâtiment, le cas des intempéries est spécifiquement prévu (article L731-1 du Code du Travail). Au delà des dispositions légales, les employeurs peuvent choisir de mettre en place une garantie de maintien de salaire en cas de situation de crise, limitée dans le temps et le cas échéant couverte par une assurance spécifique.

14.1.2 Pendant la crise

Les mesures d'urgence

Les mesures d'urgence sont mises en œuvre, dans la limite des dispositions prévues dans le cadre des contrats de travail, du règlement intérieur et de tout autre convention ou accord applicable, et dans le respect des dispositions légales et réglementaires (telles que respect des horaires, travail de nuit, travail le week-end).

14.1.3 Après la crise

Une attention particulière doit être portée aux mesures suivantes :

— mise en œuvre le cas échéant de licenciements économiques individuels ou collectif, dans le respect des dispositions légales ;

— respect des obligations déclaratives aux organismes concernés en tant que de besoin ;

— suivi spécifique en cas d'atteintes corporelles ou psychiques aux personnes, élaboration de mesures de reclassement en liaison avec les organismes de prévoyance partenaires de l'entreprise.

14.2 Éléments juridiques en rapport avec l'activité de l'entreprise

14.2.1 Avant la crise

Les aspects contractuels

Il est indispensable d'identifier préalablement à toute situation de crise les partenaires et les fournisseurs essentiels à la continuité de l'activité de l'entreprise, notamment dans le domaine des infrastructures informatiques et télécoms, dans le domaine logistique, ou tout autre domaine nécessaire à la poursuite de l'activité de l'entreprise.

La gestion de crise doit faire l'objet de dispositions contractuelles spécifiques avec tous ces partenaires/fournisseurs, dont la mise en œuvre est régulièrement testée en dehors de toute situation de crise. Par exemple : le basculement de l'informatique et des réseaux sur un centre de secours.

L'audit de la couverture d'assurance

Les polices d'assurance dommage et d'assurance responsabilité civile professionnelle, et perte d'exploitation doivent être auditées à la lumière des conséquences pour l'entreprise d'une crise majeure, tant au regard des biens et des personnes dont elle a la charge que dans l'éventualité des recours des tiers en cas d'impossibilité pour l'entreprise de remplir ses engagements vis à vis de ses clients. La plupart des polices ne couvrant pas les conséquences des actes de guerre, de terrorisme ou de catastrophes naturelles, cette analyse permet à l'entreprise d'évaluer préalablement son risque financier et de souscrire, le cas échéant, des garanties particulières ou d'anticiper un secours bancaire.

La conformité aux règles de «compliance»

De nombreuses réglementations régissent le comportement des entreprises, les unes d'ordre général (Sarbanes-Oxley, loi de sécurité financière, loi de 1978 sur la protection des données personnelles) et d'autres dépendant du secteur d'activité. Une crise peut avoir pour conséquence de révéler une faiblesse majeure dans la conformité de l'entreprise à ces règles ce qui, en plus des conséquences subies directement par l'entreprise, pourrait se traduire par l'application de la sanction prévue en cas de non conformité.

14.2.2 Pendant la crise

Constat et sauvegarde des éléments de preuve

Beaucoup d'entreprises se privent de moyens de réparation importants lors de l'occurrence d'un sinistre, car de nombreuses preuves permettant de caractériser et de chiffrer celui-ci ne sont pas constituées et sauvegardées. Il est indispensable de disposer d'éléments de preuve, tant vis-à-vis d'une éventuelle couverture par l'assurance qu'aux fins d'exercer le cas échéant des recours contre des tiers identifiés ayant une responsabilité dans le sinistre.

À cet effet, il ne faut pas hésiter à recourir aux services d'un huissier territorialement compétent afin d'établir un constat accompagné de photographies et de vidéos. En cas d'impossibilité de recours à un huissier et en tout état de cause avant l'arrivée de celui ci, l'entreprise doit procéder par elle-même à ces enregistrements de preuves. En cas de poursuite au pénal contre un tiers impliqué dans le sinistre, tous les éléments de preuve sont recevables quel que soit le moyen par lequel ils ont été collectés.

Relations avec les fournisseurs et les clients

L'occurrence de la crise doit faire l'objet d'une information immédiate, par tous moyens, des fournisseurs et des clients. Cette information permet aux co-contractants de l'entreprise de prendre eux mêmes les mesures conservatoires qui s'imposent et de diminuer leur préjudice (et par voie de conséquence le montant des recours exercés envers l'entreprise qui subit la situation de crise).

Si la crise peut être qualifiée de cas de force majeure, la date de début de l'empêchement doit être notifiée au cocontractant car elle fait partir le délai pendant lequel les obligations de l'entreprise sont suspendues. Il est à noter que la «force majeure» peut revêtir différentes acceptations : si le contrat ne la précise pas, elle est définie par la jurisprudence des tribunaux (événement extérieur, irrésistible, imprévisible) ; souvent, les contrats donnent des définitions contractuelles plus larges de la force majeure, qui incluent la grève, les intempéries, les actes de terrorisme, etc.

Vis-à-vis des fournisseurs, un certain nombre de mesures immédiates doivent être prises, selon le contexte. Par exemple : suspension ou annulation des commandes en cours, négociation d'un moratoire de paiement pour éviter l'accumulation des intérêts de retard.

Vis-à-vis des clients, les mesures à prendre dépendent de la criticité pour le client de la fourniture de produits ou de prestation qui a été interrompue. Le cas échéant, l'entreprise peut d'elle même proposer une solution alternative, qui offre l'avantage d'être maîtrisée par elle et donc moins coûteuse qu'une annulation de commande ou un remplacement d'office par le client.

La mise en cause du (ou des) tiers responsable(s) de la rupture d'activité

Dans certaines circonstances, la rupture d'activité est imputable à un ou plusieurs tiers identifiés, avec lesquels l'entreprise est liée ou non par un contrat.

Aux fins de maximiser l'efficacité d'un recours contre le tiers responsable, la faute et le préjudice en résultant doit lui être immédiatement notifié, tous droits de l'entreprise étant bien entendu réservés dans la perspective d'une évaluation définitive du préjudice.

La déclaration d'assurance

Le sinistre doit être déclaré aux assureurs dans les délais prévus.

14.2.3 Après la crise

Bilan contractuel fournisseur

La situation doit être envisagée fournisseur par fournisseur, et le cas échéant les dédommagements seront négociés : conséquences des annulations de commande, applicabilité de l'exonération de responsabilité de l'entreprise pour force majeure, accord sur un moratoire de paiement ou un échelonnement des commandes.

Bilan contractuel client

La situation doit être envisagée client par client, en fonction du préjudice subi par le client et des dispositions contractuelles : applicabilité de l'exonération de responsabilité de l'entreprise pour force majeure, clause limitative de responsabilité. Le cas échéant, il peut être proposé au client de conclure un avenant permettant de prendre en compte le caractère exceptionnel de la situation et un plan de retour à la normale.

À cet égard, il serait intéressant d'introduire dans les contrats clients des clauses spécifiques «Rupture d'activité» par lesquelles le client accepterait lors de la conclusion du contrat la possibilité de négocier un avenant en cas d'occurrence d'un sinistre ayant des conséquences sur la continuité de l'activité de son fournisseur. Ces clauses, identiques dans l'esprit aux clauses dites de «hardship», permettraient de prendre en compte les risques d'une nature nouvelle liés à certains types de catastrophes modernes. Elles sont pour l'instant peu fréquentes dans la pratique contractuelle, mais pourraient être élaborées à l'occasion de la généralisation de l'adoption par les entreprises de plan de continuité d'activité.

Suivi juridique global

Une situation de crise est susceptible d'entraîner un accroissement inhabituel du volume de réclamations et de litiges, que ce soit en demande ou en défense. Il est souhaitable de mettre en place une cellule de suivi spécifique de ces réclamations et litiges, incluant la relation avec les assureurs et les avocats.

15 Gestion de la documentation (méthode et outils)

Le choix de la gestion de la documentation dépend de plusieurs facteurs et doit être examiné en conséquence selon les trois critères suivants : confidentialité, criticité, accessibilité.

Avant de définir l'environnement relatif à la gestion de documentation, il convient d'étudier :

- Les informations, procédures, modèles types à mettre à disposition des services/acteurs ;
- Le nombre de documents PCA à produire ou déjà produits (volumétrie) ;
- Les droits en lecture, en modification ;
- Les modes et supports de stockage.

Il est essentiel de faire en sorte de :

- retenir des outils de mises à jour sans contraindre l'organisation existante (exemple : ne pas réinventer l'existant de l'organisation, ni créer des doublons de documents,..),
- permettre l'accès à toutes ces informations depuis le(s) site(s) de secours / repli utilisateurs.

On peut utiliser des outils/supports bureautiques respectant des critères de confidentialité, criticité et accessibilité, tels que :

- Word, Excel, Access, autres ;

sur des supports comme, par exemple :

- Clé USB, CD-ROM, Mini classeur papier, autres.

Il existe également sur le marché des logiciels de gestion de la documentation d'un PCA.

Les règles spécifiques de la gestion de la documentation doivent s'appliquer aux partenaires impliqués dans le PCA (fournisseurs, prestataires, etc.), dès lors que ces derniers l'utilisent.

Les modes d'accessibilité et de mise à disposition des documents diffèrent d'une entreprise à l'autre.

On constate, notamment dans le cadre de la gestion d'une crise, que les entreprises ayant développé leurs PCA au delà des classements dans des dossiers ou bases spécifiques, ont mis en place un environnement «Intranet / Extranet PCA», le plus souvent interactif (échanges de données, problématiques PCA entre les différents coordinateurs de projet métiers, site, pays). Notons que ce type de solution présente l'avantage d'être accessible depuis n'importe quel accès Internet et à n'importe quel moment de la journée.

L'annuaire de gestion de crise :

Ce document présente et répertorie la liste exhaustive des personnes à contacter en cas d'activation du PCA. Il apporte également d'autres informations comme par exemple :

- un résumé des procédures d'escalade ;
- la liste des outils /moyens mis à disposition des membres de la cellule de gestion de crise en fonction de l'incident ou du sinistre (site de repli utilisateurs, site de secours informatique, salles de réunion, etc.) ;
- la liste des suppléants, etc.

L'annuaire, dans certain cas baptisé sous le nom «l'indispensable PCA», est accessible depuis l'Intranet/Extranet. Il doit également être réalisé au format papier, ou sous tout autre type de support (CD, clé USB,..). Sa mise à jour régulière est fortement recommandée, notamment dans le cadre d'un changement d'organisation.

16 Coûts et Financement du PCA

16.1 Coûts du PCA

Il convient de distinguer au moins 5 différentes étapes :

1) le coût du «projet PCA» ;
2) le coût initial (investissements) des solutions pour assurer la continuité des activités ;
3) le coût additionnel d'exploitation, dû à la mise en place du PCA (hors crise) ;
4) le coût récurrent (charge annuelle) pour maintenir le PCA opérationnel ;
5) le coût du déclenchement du PCA lorsque l'inaccessibilité à l'environnement de travail survient.

16.1.1 Le coût «du projet» PCA

La définition du PCA, sa matérialisation (rédaction de la stratégie de continuité, des procédures), et la formation du personnel doivent être financés par une ligne budgétaire spécifique qui se traduit par la somme des charges de travail internes de l'équipe projet (coordinateur, relais PCA) et des équipes techniques, responsables des métiers et des fonctions critiques, et le cas échéant les budgets alloués aux prestataires.

16.1.2 Le coût initial

La mise en place des solutions va générer des frais d'investissements initiaux en général amortissables sur plusieurs années.

Exemples :

— Réalisation d'un site de repli utilisateurs en interne avec aménagement d'un ou plusieurs espaces ;

— Modifications du PCIT pour couvrir la stratégie de continuité :

- Installation de nouvelles liaisons télécoms ;
- Nouveaux serveurs de back up ;
- Achats de licences supplémentaires.

Il convient de prévoir également la somme des charges de travail des équipes techniques pour mettre en œuvre les investissements initiaux.

16.1.3 Le coût additionnel d'exploitation

Dans certain cas, le PCIT nécessite que l'on duplique/double quelques unes des ressources informatiques dont on veut assurer la continuité. Ceci engendre, au delà du coût d'investissement à prévoir, un coût additionnel d'exploitation directement lié aux personnels additionnels en charge de surveiller, configurer, mettre à niveau, ces nouvelles ressources.

16.1.4 Le coût récurrent

Les coûts récurrents annuels les plus apparents sont en principe les redevances annuelles payées aux prestataires offrant un environnement de travail de secours (site de repli utilisateurs et/ou site de secours informatique). Il faut cependant a minima y ajouter :

- Les abonnements télécoms des liaisons entre les différents sites de secours ;
- La charge de travail de l'équipe projet ou le budget du prestataire qui met à jour les procédures ;
- La charge de travail des équipes qui participent à la préparation et à la réalisation du test annuel regroupant à la fois les équipes techniques, les métiers et les fonctions critiques.

16.1.5 Le coût du déclenchement

Le coût du déclenchement du PCA peut être approché par une analyse qui reste cependant une évaluation : personne ne sait quelle sera l'ampleur du sinistre, ni la période à laquelle il surviendra, ce qui d'emblée crée des inconnues significatives.

Cette section ne prend pas en compte l'évaluation des frais relatifs à la reconstruction d'un site sinistré.

Certains frais sont cependant déjà connus et d'autres peuvent être évalués :

- Le coût initial du déclenchement et/ou le coût d'occupation à la journée facturée par le prestataire de secours offrant un environnement de travail de secours ;
- L'évaluation du coût des éventuelles primes hebdomadaires ou mensuelles versées au personnel travaillant sur les sites de secours ;
- L'évaluation des coûts mensuels des communications depuis le site de secours ;
- Le coût des commissions ou frais que dans certaines entreprises on ne facturera pas aux clients à cause du retard généré par l'interruption de service.

16.2 Financement du PCA

Il existe peu de données quant au financement du PCA par les entreprises.

Le PCA fait parfois encore partie des budgets informatiques (prolongement des budgets consacrés au PCIT), ou bien, dans certains cas, il est rattaché à une ligne budgétaire spécifique créée soit par la Direction Générale, soit par la Direction Financière.

Les charges de travail consacrées par les équipes internes pour développer et tester le PCA sont encore peu identifiées et comptabilisées comme telles.

La grande majorité des entreprises finance le PCA avec sa propre trésorerie [4)].

Rares sont les entreprises qui ont recours à un financement extérieur.

Comme évoqué dans le chapitre «les aspects juridiques» (section audit de la couverture assurance), une partie des frais liés au déclenchement du PCA peut être prise en compte dans la partie «frais supplémentaires» des entreprises ayant souscrit une assurance «pertes d'exploitation».

Pour faire prendre en compte par les compagnies d'assurance le financement des frais supplémentaires «Déclenchement PCA», le responsable du projet PCA travaille en collaboration avec le responsable des assurances ou Risk Manager pour définir et évaluer les frais supplémentaires.

En cas de déclenchement du PCA, il est courant de faire prendre en charge par la compagnie d'assurance une partie des frais journaliers facturés (voir franchise et couverture maximum de la police souscrite) par le prestataire offrant le site de repli . Il faut cependant avoir préalablement fait figurer ces frais dans le contrat d'assurance.

Nous n'évoquons pas ici les différentes assurances «dommages» que l'entreprise souscrit naturellement pour se couvrir de la perte de son environnement de travail. Cependant il est recommandé au niveau technique de réévaluer régulièrement la valeur du matériel informatique et télécom.

Notons qu'en Angleterre et aux USA certaines entreprises réussissent à faire réduire leurs primes d'assurance en fournissant aux compagnies la garantie que leur PCA est opérationnel.

---

4) Une étude du CLUSIF concernant les seuls PCIT précise qu'en 2002 86% des entreprises finançaient leur PCIT avec leur propre trésorerie.

17 Résumé

Le périmètre des activités vitales traitées dans le cadre d'un PCA dépend directement des impacts liés aux pertes de l'entreprise, et qui peuvent être de natures différentes :

- Réglementaires (Bâle II, CRBF 97/02, …) ;
- Financières (pertes de revenus, retards de trésorerie, coûts supplémentaires imprévus liés à la crise, diminution de la valeur de l'action…) ;
- Opérationnelles (pertes de stocks ou de production, retard de livraison, …) ;
- Image (pertes de part de marché, image auprès des clients, …) ;
- Contractuelles et juridiques (pénalités, plaintes des clients,…) ;

La définition du périmètre et le contenu du PCA sont des choix stratégiques du ressort de la Direction Générale. Certains risques peuvent être néanmoins couverts par un tiers (hébergeur, assureur, etc.).

L'organisation et la mise en œuvre du PCA découlent de ces choix stratégiques et doivent aborder les thèmes suivants :

- La gestion de la crise ;
- La continuité des métiers (PCO) ;
- La continuité de l'Informatique et des Télécommunications (PCIT) ;
- Les exercices de test et la formation ;
- Le Maintien en Condition Opérationnelle (MCO) ;
- Le Retour à la situation nominale ;
- Les aspects juridiques ;
- La gestion de la documentation.

Il est peu vraisemblable d'envisager un retour instantané de toutes les activités à une situation nominale. Le PCA adresse principalement la survie et la pérennité de l'organisation, en reprenant prioritairement ses activités sensibles afin de limiter leurs pertes, jusqu'à un niveau jugé acceptable par les instances décisionnelles.

Le PCA ne couvre pas tous les risques de pertes liés à un sinistre.

Le PCA est un moyen, non une finalité.

18 ANNEXES

18.1 Quelques chiffres et statistiques

Coût estimé des arrêts de production

En 2005, une étude auprès de 80 grandes compagnies a démontré que le coût estimé des arrêts de production dû à la perte de données serait de l'ordre de 3,6 % de leur revenu annuel.

(Source Infonetics research).

Impact d'une perte de données (secteur bancaire)

70 % des entreprises ayant subi une perte de données majeure ne survivent pas plus de 18 mois.

(Source UK : Departement Of Trade Industry).

Indisponibilité du centre informatique

93 % des entreprises dont le centre informatique reste inexploitable pendant 10 jours ou plus suite à un sinistre déposent le bilan dans l'année suivant le sinistre.

(Source NARA : National Archives & records Administration, Washington).

Tentatives de recouvrement de données

Des analystes ont estimé que 40 % des recouvrements de données échouaient.

(Source ESG : Entreprise Strategy Group).

Capital intellectuel

Jusqu'à 70 % du capital intellectuel des entreprises sont stockés sur des PC et/ou des portables.

(Source Infonetics research)

18.2 Glossaire

Accidents — Toute atteinte dont l'origine est en général liée à des éléments naturels, ou à certaines causes de nature involontaire. Les conséquences dues aux accidents sont tangibles et se manifestent surtout sur l'environnement physique.

Traduction anglaise : **Accidents.**

Activité — Ensemble de processus qui concourent à la réalisation d'objectifs bien définis.

Traduction anglaise : **Business, Activity**

Activité critique — Activité qui, en cas d'interruption, doit être rétablie pour éviter à l'entreprise des pertes trop importantes ou d'autres impacts préjudiciables à la survie de l'entreprise.

Traduction anglaise : **Critical business**

Analyse de risque — Identification des risques auxquels une entreprise est exposée, évaluation éventuelle de la probabilité d'occurrence d'un sinistre, détermination des activités critiques dont la continuité est essentielle, définition des contrôles nécessaires à la réduction du niveau de risque et estimation du coût correspondant.

Utilisation systématique d'informations pour identifier les sources et pour estimer le risque.

> NOTE 1 L'analyse du risque fournit une base à l'évaluation du risque, au traitement du risque et à l'acceptation du risque.
>
> NOTE 2 Les informations peuvent inclure des données historiques, une analyse théorique, des opinions justifiées, et des préoccupations des parties prenantes.

Source ISO/IEC Guide 73:2002

Traduction anglaise : **Risk analysis**.

Annuaire de gestion de crise — Document complet d'information nécessaire en cas d'activation de PCA.

Autre dénomination : **L'indispensable PCA**

Traduction anglaise : Directory of crisis management

Attaque — Concrétisation d'une menace qui provoquera une atteinte sur l'environnement physique, logique ou organisationnel de la donnée et/ou de l'information. Les mesures de sécurité retenues pour lutter contre l'agression seront la dissuasion et, à un niveau plus fort, la protection dont le premier objectif sera de détecter l'agression, de tenter de la neutraliser ou à défaut d'en atténuer les effets.

Autre dénomination : **Agression**

Traduction anglaise : **Aggression, Attack**

Bilan d'Impact sur les Activités (BIA) — Détermination des impacts sur une entreprise d'une interruption d'activité faisant suite à un sinistre. Les impacts à considérer devraient porter aussi bien sur les pertes financières que sur l'image de l'entreprise, ses obligations réglementaires et juridiques, ses contraintes sociales et organisationnelles.

Autres dénominations : **Analyse d'impact sur les activités / Analyse d'impact sur les affaires**.

Traduction anglaise : **Business Impact Analysis (BIA)**.

Cellule de Crise — Elle est composée des responsables de chaque Direction utilisatrice concernée par le PCA. Elle comprend également des membres de la Direction Générale, de la Direction des Services Généraux, de la Direction des Ressources humaines, de la Direction de la Communication, de la Direction Informatique et des responsables PCA. Son rôle est de se réunir en cas d'incident grave pour décider de déclencher ou non le PCA. Ses membres doivent être assujettis à des astreintes (service de garde) ou au moins être disponibles à tout moment et en tout lieu.

Autre dénomination : **Comité de crise**.

Traduction anglaise : **Crisis Team**.

Centre de gestion de Crise — Site où la Cellule de Crise se réunit afin de gérer la crise.

Conséquence — Résultat d'un événement.

NOTE 1 Il peut y avoir plus d'une conséquence d'événement.

NOTE 1 Les conséquences peuvent englober des aspects positifs et des aspects négatifs. Cependant, les conséquences sont toujours négatives pour les aspects liés à la sécurité.

NOTE 2 Les conséquences peuvent être exprimées de façon qualitative ou quantitative.

Source ISO/IEC Guide 73:2002

Répercussion de l'effet, au second degré, sur d'autres plans, qui pourront être successivement de niveaux : physiques (destruction matérielle), logiques (atteinte organisationnelle), puis conceptuels (atteinte stratégique, pertes financières ou réalisation d'enjeux).

Traduction anglaise : **Consequence, Effect.**

Contamination — Détérioration de matériels due à un incendie, un dégât des eaux ou tout autre sinistre du même type.

Continuité de service informatique — Disponibilité en temps réel du système d'information en cas de sinistre grâce à la réplication totale des ressources informatiques.

Autre dénomination : **Haute-disponibilité**.

Traduction anglaise : **Hot back-up**.

Correspondant PCA — Personne en charge du PCA pour une activité donnée et qui rend compte au Coordinateur PCA ou RPCA de l'entreprise.

Crise — Événement soudain causant des pertes et des dommages importants, entrainant une interruption d'une ou plusieurs activités critiques ou un arrêt de l'organisme, ayant des impacts à long terme et nécessitant le recours à la Cellule de Crise et, le cas échéant, à un site alternatif. Une crise peut avoir des conséquences sur la survie même de l'entreprise.

Traduction anglaise : **Crisis**.

Durée d'Indisponibilité Maximale Admissible (DIMA/DMIA) — Pour une activité ou un processus donné, délai admissible d'interruption avant qu'il y ait un impact grave et au-delà duquel la reprise est nécessaire.

C'est le délai total nécessaire entre l'arrêt de l'activité et la remise à disposition du système d'information aux utilisateurs.

Autre dénomination : **Objectif de délai de reprise**.

Traduction anglaise : **Recovery Time Objective (RTO)**.

Enjeu — Ce que l'on peut perdre ou gagner. Ils peuvent être de différents niveaux. L'enjeu majeur de l'entreprise sera le dépôt de bilan.

Traduction anglaise : **Stake.**

Événement déclencheur — Origine d'un sinistre susceptible d'amener la Cellule de Crise à décider de déclencher l'exécution du PCA.

Incident — Événement, anticipé ou non, qui perturbe le cours normal des activités économiques de l'organisation, ayant un faible impact sur l'organisme et des conséquences potentielles à court et moyen termes sur la continuité des activités essentielles de l'organisme. Un incident, s'il n'est pas maîtrisé peut entraîner une crise. On rencontre des incidents tous les jours.

Traduction anglaise : **Incident.**

Manuel de Cellule de Crise — Ensemble des procédures permettant à la Cellule de Crise de gérer une crise suite à un sinistre.

Menace — Événement qui peut transformer un risque en perte. Une menace est un phénomène naturel comme une crue ou un séisme, ou un incident d'origine humaine comme un attentat, un virus informatique, une panne de courant ou encore un sabotage dû à un employé mécontent.

Traduction anglaise : **Threat**.

Mesures d'urgence — Dispositions ayant pour objectif de contenir les effets immédiats et à court terme du sinistre.

Autre dénomination : **Premières mesures**.

Plan de Continuité d'Activité (PCA) — Ensemble des procédures et dispositions prévues pour permettre à l'entreprise de réagir face à un sinistre, de manière à garantir la reprise de ses activités critiques.

Autres dénominations : **Plan de secours / Plan de Continuité des Affaires (PCA) / Plan de contingence**.

Traduction anglaise : **Business Continuity Plan (BCP) / Business Contingency Plan (BCP)**.

Perte de Données Maximale Admissible (PDMA) — Pour une application quelle est la perte acceptable au niveau des données (liée aux sauvegardes) pour que celle-ci soit d'un niveau acceptable pour les services utilisateurs.

Selon les besoins exprimés, le degré de fraîcheur des données correspond à la perte des données considérées comme acceptable entre l'arrêt de l'activité et sa reprise. Par exemple, au démarrage après sinistre, les données peuvent dater de la veille au soir, du matin ou de la minute du sinistre.

Autres dénominations : **Degré de fraîcheur des données**.

Traduction anglaise : **Recovery Point Objective (RPO)**.

Planification de la Continuité d'Activité — Élaboration des procédures et déploiement des moyens permettant à l'entreprise de réagir face à un sinistre, de manière à garantir la reprise de ses activités critiques.

Le Comité de Réglementation Bancaire et Financière impose aux établissements de crédit et aux entreprises d'investissement de disposer d'un plan global réunissant l'ensemble des PCA qui soit objectivé et régulièrement évalué sous le contrôle de l'organe délibérant de l'organisation (article 1 du règlement CRBF 2004-02).

Autres dénominations : **Planification de la continuité des affaires**.

Traduction anglaise : **Business Continuity Planning (BCP) / Business Contingency Planning (BCP)**.

Plan de Continuité Informatique et Télécom (PCIT) — Ensemble des procédures et dispositions prévues pour garantir à l'entreprise la reprise de son système informatique en cas de sinistre.

Sous-ensemble du PCA qui couvre les moyens informatiques et télécom. Il garantit la reprise des systèmes désignés comme critiques dans le temps minimum fixé.

Autre dénomination : **Plan de Secours Informatique (PSI)**.

Traduction anglaise : **Disaster Recovery Plan (DRP)**.

Plan de Continuité des Opérations (PCO) : Le Plan de Continuité des Opérations couvre la perte des locaux des utilisateurs conduisant au repli des utilisateurs sur un autre site.

Autre dénomination : **PRU : Plan de Repli Utilisateurs**.

Traduction anglaise : **Business Continuity Plan (BCP)**.

Plan de sécurisation — Ensemble des procédures et dispositions permettant de réduire les risques d'exposition de l'entreprise à un sinistre d'origine interne voire externe.

Plan de test — Il permet dans un premier temps de valider ce qui a été mis en place par rapport aux besoins exprimés. Puis, à intervalle régulier, il permet de garantir le caractère opérationnel du PCA.

Périmètre de sécurité — Zone délimitée par les autorités publiques suite à un sinistre, dont l'accès est interdit au public pour des raisons de sécurité.

Point critique — Une ressource ou une source unique de service, activité, et/ou processus. Typiquement, il n'y a aucune alternative et une perte de cet élément pourrait mener à l'échec d'une fonction critique.

Traduction anglaise : **Single point of failure**.

Point de ralliement — Lieu où doivent se rendre les personnes concernées dès la survenance d'un sinistre.

Position de travail — Ensemble formé par un bureau, un poste de travail (PC) et un téléphone. Elle peut être définie en fonction des spécificités de l'entreprise.

Traduction anglaise : **Workstation**.

Procédures d'escalade — Document répertoriant séquentiellement, par activité, les différents types d'incidents et de crises par niveaux de gravité, les conditions d'escalade, ainsi que les indicateurs, les responsables et les plans de continuité associés. La procédure d'escalade pointe sur l'annuaire d'alerte et de gestion de plan de continuité. Il devrait être à la disposition de la cellule de crise.

Traduction anglaise : **escalation procedures.**

Procédures techniques — Elles décrivent les actions à faire par la Direction Informatique au quotidien pour garder les moyens techniques de secours à jour. Elles décrivent également les actions à faire en cas d'activation de PCA ou à l'occasion des tests. Elle est écrite par la Direction Informatique.

Traduction anglaise : **Technical procedures, Operational procedures**.

Processus critique — Processus qui, en cas d'interruption, doit être rétabli pour éviter à l'entreprise des pertes trop importantes ou d'autres impacts préjudiciables.

Proposition de Solutions de Secours (PSS) — Document recensant les solutions de secours à envisager dans le cadre du développement d'un PCA.

Résilience — Capacité d'une organisation à résister à un incident, à un accident, à une crise dans des environnements adverses, puis à revenir à un état normal.

Traduction anglaise : **Resilience**.

Responsable de Plan — Personne en charge du PCA pour une direction ou un département donné et qui anime l'ensemble des correspondants PCA sous sa responsabilité. Il rend compte au responsable du PCA de l'entreprise.

Traduction anglaise : **Plan Manager**.

Responsable du PCA (RPCA) — Coordinateur PCA au niveau entreprise ou groupe.

Autre dénomination : **Coordinateur PCA.**

Traduction anglaise : **Business Continuity Manager / Business Continuity Coordinator / BCP Manager**.

Retour à la normale — Capacité d'une entreprise, après un choc extrême, à accepter et traiter de nouvelles opérations, à un rythme au moins égal à celui précédent la catastrophe.

Autre dénomination : **Situation nominale**.

Traduction anglaise : **Resumption**.

Salle blanche — Site de secours sans ressources ni équipement, sauf la climatisation et le câblage électrique.

Autre dénomination : **Site de reprise non-équipé**.

Traduction anglaise : **Cold site**.

Salle de réunion de la cellule de crise — Désigne l'endroit où la cellule de crise se réunit en cas de nécessité. Il est situé dans un périmètre proche de l'environnement ciblé par le PCA mais ne doit pas être adjacent à celui-ci. Il est en général équipé d'au minimum un téléphone, un fax, un PC et une armoire ignifuge dans laquelle se trouvent les procédures du PCA.

Autre dénomination : **Centre de gestion de crise**

Sinistre — Événement soudain, imprévu et grave, causant d'importants dommages ou plaçant l'entreprise dans l'incapacité d'accomplir ses activités critiques.

Autre dénomination : **Désastre**.

Traduction anglaise : **Disaster**.

Site primaire — Site principal de l'entreprise, devant être secouru.

Autre dénomination : **Site de production**.

Traduction anglaise : **Primary site**.

Site de secours — Site, autre que le site primaire, pouvant être utilisé pour héberger des activités critiques de l'entreprise.

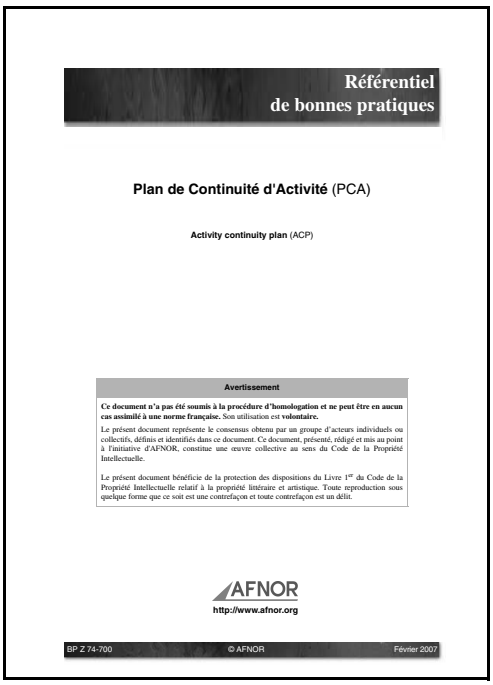
Autres dénominations : **Site de repli / Site de reprise / Site alternatif / Centre de secours**.

Traduction anglaise : **Recovery site**.

Solution de secours — Organisation et ensemble des moyens mis en place pour parer à un éventuel sinistre.

Stockage hors-site — Stockage délocalisé sur un site assez éloigné du site primaire, permettant de conserver du matériel, des documents et autres supports de données indispensables en cas de sinistre.

Tests — Ils permettent dans un premier temps de valider ce qui a été mis en place par rapport aux besoins utilisateurs sur la solution de continuité. Puis, à intervalle régulier, ils permettent de garantir le maintien opérationnel du PCA.



Le présent document a pour objet la continuité de l'activité métier de l'entreprise qui est d'assurer la continuité des services critiques rendus à ses clients ; il présente les bonnes pratiques en matière de PCA (plan de continuité d'activité) dans des situations à risques pendant ou après un sinistre.

Mots-clés entreprise, sécurité, gestion, risque, prévention, mesure d'urgence, organisation, information, mise en oeuvre, schéma, niveau, formation, informatique, télécommunication, logistique.

FA151795 ISSN 0335-3931

ICS : 03.100.01 ; 13.200 ; 35.020