Mémoire de Fin d'Etudes
Msc Audit et Gouvernance des Organisations

DERRAHI Meriem

GARCIA Jordane

2013

GUIDE D'AUDIT

L'audit des Plans de Continuité d'Activité et de la Gestion de Crise

Analyse Comparative Sectorielle

Sommaire

Remerciements 4
Benchmark 5

Introduction 6
Contexte actuel 6
De l'intérêt d'une démarche PCA 6
Présentation du travail réalisé 8

1. Le PCA : Définition, contexte et bonnes pratiques 9
1.1 Définition 9
1.2 Règlementation et normes 11
1.2.1 Référentiel normatif générique 11
1.2.2 Cadre législatif et règlementaire spécifique 12
1.3 La mise en place d'un PCA : Référentiel générique des bonnes pratiques 20
1.3.1 La conception du PCA 20
1.3.2 La mise en œuvre du PCA : Le déploiement 40
1.3.3 La maintenance du PCA 50
1.4 Spécificités sectorielles de mise en place d'un PCA et d'une gestion de crise 53
1.4.1 Secteur bancaire 53
1.4.2 Secteur de la santé publique 53
1.4.3 Secteur alimentaire 54
1.4.4 Secteur de l'énergie 55
1.4.5 Secteur des transports 55
1.4.6 Secteur des télécommunications 56
1.5 Les outils 57
Synthèse de la première partie 58

2. Les risques associés aux plans de continuité d'activité 59
2.1 Risques majeurs d'indisponibilité de l'environnement de travail (Génériques) 59
2.1.1 Sinistres naturels 60
2.1.2 Sinistres technologiques 60
2.1.3 Sinistres sociaux, économiques et politiques 61

2.1.4 Sinistres sanitaires 61
2.1.5 Sinistres nucléaires, radiologiques, biologiques et chimiques 62
2.2 Risques d'impacts liés aux points de contrôle clés de continuité (Génériques) 63
2.2.1 Risques liés à la conception du PCA 63
2.2.2 Risques liés au déploiement du PCA 69
2.2.3 Risques liés à la maintenance du PCA 72
2.3 Risques spécifiques sectoriels 73
2.3.1 Secteur bancaire 73
2.3.2 Secteur de la santé publique 74
2.3.3 Secteur alimentaire 76
2.3.4 Secteur de l'énergie 78
2.3.5 Secteur des transports 79
2.3.6 Secteur des télécommunications 81
2.4 Quelques exemples de sinistres célèbres 83
2.4.1 Catastrophes naturelles 83
2.4.2 Sinistres technologiques 83
2.4.3 Sinistres sociaux, économiques, politiques 83
2.4.4 Crises sanitaires 83
2.4.5 Sinistres nucléaires, radiologiques, biologiques ou chimiques 84
2.4.6 Zoom sur un retour d'expérience de Benchmark : Accident nucléaire de Fukushima (11/03/2011, Japon) 84
2.5 L'Articulation avec les autres dispositifs de maîtrise des risques 86
2.5.1 Articulation avec le Management des Risques 86
2.5.2 Articulation avec les assurances 86
2.5.3 Articulation avec les autres volets du Contrôle Interne 86
2.5.4 Articulation avec l'Audit Interne 87
2.5.5 Charte du PCA 87
Synthèse de la seconde partie 88

3. Guide d'audit des plans de continuité d'activité 89
3.1 Objectif de l'Audit des PCA 90
3.2 Méthodologie générale 90
3.3 Guide d'Audit des PCA : Référentiel Générique 92
3.3.1 La conception du PCA 92

3.3.2 Le déploiement du PCA 99
3.3.3 La maintenance du PCA 106
3.4 Référentiels spécifiques sectoriels 110
3.4.1 Secteur bancaire 110
3.4.2 Secteur de la santé publique 112
3.4.3 Secteur alimentaire 114
3.4.4 Secteur de l'énergie 116
3.4.5 Secteur des transports 118
3.4.6 Secteur des télécommunications 121

Conclusion 123
La réalité des PCA en quelques chiffres 123
Conclusion générale et perspectives 125

Annexes 126
Annexe 1 – Sources documentaires 126
Supports de formation 126
Ouvrages 126
Articles et publications 126
Normes, lois et règlements 126
Sites Internet 129
Annexe 2 – Glossaire 130
Annexe 3 – Répertoire des Acronymes 132
Annexe 4 – Comptes-rendus des entretiens de Benchmark 135

L'Audit des Plans de Continuité d'Activité et de la Gestion de Crise

Remerciements

« Ce mémoire n'aurait pas pu voir le jour sans l'intervention d'un grand nombre de personnes. Nous souhaitons ici les remercier d'avoir chacun à leur façon contribué à nos travaux.

Nous tenons tout d'abord à remercier très chaleureusement l'équipe du Club de Continuité d'Activité. Les conseils qu'ils nous ont prodigués, ainsi que la confiance qui nous a été accordée en nous mettant en contact avec le réseau, ont été déterminants dans la réalisation de notre travail de recherche et la bonne marche de notre Benchmark sectoriel.
Nous les remercions particulièrement d'avoir consenti à diffuser notre questionnaire de benchmark auprès des membres du club.

Nous remercions l'ensemble des entreprises et organisations, tous secteurs d'activités confondus, qui ont participé à nos investigations. Merci à elles d'avoir pris le temps de nous recevoir et de répondre à nos questions. Leur participation à nos recherches et leurs retours d'expériences ont donné une autre dimension à notre analyse, la rendant beaucoup plus riche. Nos échanges avec eux nous ont par ailleurs permis d'avoir une vision très précise sur les tendances réelles actuelles.

Nous remercions également nos équipes respectives pour leur patience, leur compréhension et leurs nombreux conseils. Merci à nos chargés de plans de continuité d'activité d'avoir également participé à notre étude.

Nos remerciements s'étendent naturellement à tous nos enseignants, et en particulier à Messieurs Billot et Vera qui nous ont accompagnées et guidés durant toute cette année et à qui nous sommes très fières de présenter nos travaux.

Merci au réseau IAE, à nos camarades et à tous ceux qui, de près ou de loin, ont contribué à la réalisation de ce mémoire.

Bonne Lecture. »

Benchmark

Entretiens

Continuité d'Activité

Secteurs d'Activité Critiques (fournisseurs de services vitaux)

Bancaire
Santé Publique
Energie
Transport
Télécommunications

Autres secteurs d'activité

Industrie Automobile
Finances Publiques
Organisation Internationale

Réponses au questionnaire

Bancaire
Assurantiel
Vins et Spiritueux
Energie
BTP
Informatique
Industrie

Dans un souci de respect de la confidentialité des informations, les organisations et interlocuteurs ayant participé à notre étude ont préféré garder l'anonymat.

Introduction

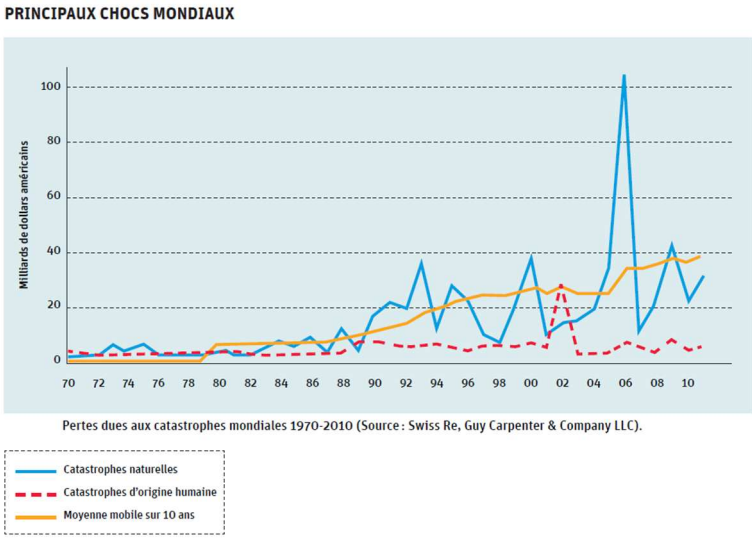
Contexte actuel

Les problématiques liées à la continuité d'activité sont aujourd'hui essentielles pour les organisations, quels que soient leur type, leur taille et leur secteur d'activité. En ces temps de crise financière et de multiplication des risques majeurs tels que le terrorisme ou les catastrophes naturelles, et où la mondialisation des marchés et l'interdépendance accrue des acteurs économiques renforcent leur vulnérabilité à ces évènements, elles doivent s'interroger sur leur capacité à gérer efficacement voire à survivre aux crises.
La gestion de continuité d'activité et de crise revêt donc un caractère incontournable, et devient un principe primordial de gouvernance et de saine gestion. La mise en place d'un Plan de Continuité d'Activité constitue avant tout une obligation de bon sens, de plus en plus encouragée par le législateur et les régulateurs, mais également par les différentes parties prenantes liées à l'organisation.

De l'intérêt d'une démarche PCA

L'origine naturelle de la démarche PCA découle du Management des Risques, pouvant émerger à la suite d'un évènement spécifique, d'une obligation règlementaire, de l'exigence d'une partie prenante, ou encore d'une prise de conscience de la gouvernance de l'organisation. Une prise de conscience de la nécessité de cette démarche découle souvent de la peur, mais peut également être une démarche positive de recherche de continuité de l'emploi et de l'activité, avec une volonté de projet d'entreprise. Se doter d'un PCA peut en outre améliorer l'image de l'organisation, ainsi que sa valeur financière. D'une manière générale, les entreprises qui ont entamé une démarche de continuité d'activité sont plus résilientes face aux évènements déstabilisants.

En outre, le coût du risque de plus en plus important est également un facteur motivant pour une organisation à mettre en place un PCA.



Toutes les organisations peuvent se retrouver confrontées à une crise, et sans solutions de secours mises en place en amont pour la continuité d'activité sur les zones critiques, celles-ci peuvent tout perdre. Accompagner et gérer un tel évènement ne s'improvise pas, et la préparation et l'anticipation de sa survenance sont la garantie de la réactivité et de la qualité de la réponse apportée. Dans le contexte actuel, une démarche d'anticipation des sinistres par la mise en place d'un PCA et d'une gestion de crise semble ainsi incontournable.
Un état d'urgence perturbe chacun et le risque d'être dépassé par la multiplicité des tâches et le stress est réel.

L'expérience en témoigne

« Cinq entreprises sur six qui connaissent un sinistre grave sans avoir fait une démarche préalable d'anticipation et de plan de continuité d'activité, coulent. » Sonia S. (Crédit Agricole L&F).

Zoom sur une catastrophe fatale à l'activité d'une entreprise : L'explosion d'AZF en 2001

Quand l'absence de continuité conduit à la faillite de l'activité…
Nous avons tous en tête le drame survenu à l'usine AZF de Toulouse le 21 Septembre 2001. L'explosion d'un stock de nitrate d'ammonium laissé à l'abandon avait causé la mort de 31 personnes et fait plus de 2500 blessés. Outre les conséquences humaines et matérielles que l'on peut imaginer, des flots de produits toxiques ont été déversés dans la Garonne, polluant les eaux du fleuve. En Septembre 2012, la société propriétaire de l'usine et son ancien Directeur ont été reconnus coupables.
A la suite du sinistre d'AZF, le site de Toulouse, qui appartenait à une filiale du groupe Total nommée Grande Paroisse (fabricant d'engrais azotés), est définitivement fermé.

Cette catastrophe est également un bon exemple de ce qui peut se passer lorsque les risques critiques pour la continuité d'activité sont mal maitrisés.
Ici, il s'agit du contrôle de la chaîne de production dans le secteur de l'industrie chimique. Tout comme dans certains secteurs de l'énergie, un point de contrôle clé repose sur le traitement des déchets industriels et leur stockage. Une attention particulière doit être apportée lorsqu'il s'agit de produits dangereux (hautement inflammables, explosifs,…etc.).
Le stockage aléatoire et non contrôlé du nitrate a ainsi eu des conséquences dramatiques :

- Financières : Fermeture complète d'un site
- Humaines : Morts et blessés
- Environnementales : Pollution des eaux alentours
- D'image : Pour le groupe Total et la société GPN.

Ce sinistre et les impacts qu'il a pu provoquer permettent aux organisations qui en ont été témoin de remettre en question leurs propres dispositifs de maîtrise des risques, et en particulier ceux relatifs à la continuité d'activité, afin de s'assurer que cela ne leur arrive pas.

Prise de conscience récente de la nécessité de la continuité d'activité : La pandémie grippale de 2009

De nos recherches sur les sinistres marquants et de nos entretiens de Benchmark, il ressort que la pandémie grippale de 2009 fut un tournant décisif en France pour les PCA.

En effet, cette crise sanitaire a suscité beaucoup de craintes sur les marchés boursiers mondiaux, et alerté les économies sur le besoin d'anticiper les sinistres, notamment de grande envergure.
Le premier secteur touché fut le tourisme, avec une chute sans précédent des cours boursiers pour les grandes compagnies aériennes, dans un contexte économique déjà difficile. La société a pris conscience du coût économique qu'une pandémie grippale pourrait représenter (une note des experts de la Banque Mondiale avait estimé que le coût économique de la pandémie pourrait varier de 0,7 % à 4,8 % du PIB mondial).
Au-delà de la paralysie des activités économiques, ce sinistre sanitaire n'était pas sans rappeler d'autres cas similaires comme la grippe espagnole de 1918, qui avait fait entre 50 et 100 millions de morts.
Le virus H1N1, comme nous l'ont signalé plusieurs des participants à notre Benchmark, fut donc pour les organisations françaises une vraie piqûre de rappel sur la nécessité d'anticiper ce genre de crise en amont de leur survenance, et à l'origine de la mise en place d'un dispositif de gestion de crise pour beaucoup d'entre elles.

Présentation du travail réalisé

Notre travail, qui n'a pas vocation à être exhaustif, reste néanmoins complet.
Appuyé sur une solide recherche documentaire et nos connaissances personnelles, il est étayé par un benchmark multisectoriel des bonnes pratiques en termes de continuité d'activité et de gestion de crise. Il est constitué d'éléments qualitatifs approfondis pour les secteurs d'activités que nous avons jugés critiques, dits fournisseurs de services vitaux, à savoir le secteur de la banque et assurance, de la santé publique, de l'alimentation, de l'énergie, des transports, et des télécommunications. A ces recherches s'ajoute la diffusion plus large d'un questionnaire permettant de compléter cette liste avec les secteurs de l'industrie, des finances publiques et collectivités territoriales, des vins et spiritueux, du bâtiment et travaux publics, de l'informatique, etc. Nous avons donc réellement été en mesure de mener une analyse multisectorielle très riche, afin d'élaborer un guide d'audit complet et pertinent.

Perspective d'Audit Interne

Nous avons cherché, dans une première partie, à proposer une définition, un cadre et un périmètre au sujet traité, ainsi qu'un référentiel des bonnes pratiques, à la fois générique pour tout type d'organisation et spécifique aux secteurs d'activités critiques précédemment identifiés. Cette partie sert de base à la démarche d'audit interne, en ceci qu'elle constitue le référentiel par rapport auquel est évaluée la conformité du dispositif audité, et vers lequel les recommandations d'audit doivent pousser l'organisation à tendre.
Dans une seconde partie, nous avons recensé les risques génériques et spécifiques relatifs à la continuité d'activité et la gestion de crise, contre les impacts desquels un PCA vise à se prémunir, et dont l'audit interne doit vérifier la couverture.
Enfin, la troisième partie propose un guide d'audit des PCA, à la fois générique et spécifique, en rappelant les objectifs et la méthodologie générale de l'audit, puis un tableau opérationnel reprenant les composantes de contrôle interne et les objectifs d'audit, les risques et leurs points de contrôle clés, avec quelques bonnes pratiques de contrôle interne et les techniques d'audit proposées.

1. Le PCA : Définition, contexte et bonnes pratiques

1.1 Définition

Le règlement du CRBF 2004-02 définit un PCA comme un ensemble de mesures visant à assurer, selon divers scénarios de crise, y compris face à des chocs extrêmes, le maintien, le cas échéant de façon temporaire selon un mode dégradé, des prestations de service essentielles de l'entreprise puis la reprise planifiée des activités.

Le référentiel ISO, quant à lui, propose la définition suivante : « La gestion de la continuité d'activité est définie comme un processus de management holistique qui identifie les menaces potentielles pour une organisation, ainsi que les impacts que ces menaces, si elles se concrétisent, peuvent avoir sur les opérations liées à l'activité de l'organisation, et qui fournit un cadre pour construire la résilience de l'organisation, avec une capacité de réponse efficace préservant les intérêts de ses principales parties prenantes, sa réputation, sa marque et ses activités productrices de valeur. »
« Un plan de continuité a par conséquent pour objectif de décliner la stratégie et l'ensemble des dispositions qui sont prévues pour garantir à une organisation la reprise et la continuité de ses activités à la suite d'un sinistre perturbant gravement son fonctionnement normal. Il doit permettre à l'organisation de répondre à ses obligations externes (législatives, règlementaires ou contractuelles) ou internes (risque de perte de marché, survie de l'entreprise, image…) et de tenir ses objectifs. ».

Le PCA est concerné essentiellement par les risques majeurs, de grande envergure, auxquels est soumise l'organisation, et dont la survenance viendrait menacer la pérennité de l'activité, l'atteinte des objectifs stratégiques ou la conformité aux dispositions règlementaires.
En ceci, le PCA s'inscrit en dispositif de contrôle interne et de maîtrise des risques.

Dans le cadre d'un PCA, sont identifiés et analysés en termes d'impact ces risques majeurs qui viendraient priver l'organisation de tout ou partie de ses ressources, et donc de son environnement normal de travail.
Le PCA a donc pour objet d'anticiper la survenance de ces risques, sans toutefois servir à l'éviter, et de mettre en place des mesures visant à en limiter les conséquences opérationnelles, financières, juridiques et d'image. Il va par ailleurs rassurer les clients et les différentes parties prenantes liées à l'organisation sur la sauvegarde de leurs intérêts en cas de sinistre grave.

Le PCA va s'intéresser à la pérennité des activités vitales, essentielles de l'organisation, identifiées comme critiques, et ne pouvant se permettre une interruption prolongée. En cas d'indisponibilité totale ou partielle de l'environnement de travail, le PCA doit permettre la continuité de ces activités en situation dégradée, en garantissant le niveau de service minimum qu'il aura préalablement défini.
Il est constitué pour aboutir à la reprise des activités, en prévoyant la sortie de crise et de situation dégradée, et le retour progressif à un environnement normal de travail. Ce volet spécifique du PCA est présenté sous la forme d'un PRA, ou Plan de Reprise d'Activité.

La mise en place et la vie d'un PCA s'inscrivent dans une démarche de gouvernance de l'organisation, encouragé et parfois encadré par le législateur et les régulateurs. L'implication de la Direction est donc un élément clé, qui va assurer notamment la légitimité du plan à tous les niveaux de l'organisation, essentielle dans le cadre d'une démarche aussi complexe et globale. En effet, les acteurs de l'entreprise sont concernés et impliqués dans le PCA.

Concrètement, le PCA se base sur une connaissance approfondie des risques de l'organisation, ainsi que de ses processus, ses activités et ses ressources. C'est cette connaissance qui va permettre la définition des besoins en continuité, en identifiant les risques majeurs et leurs impacts, les activités critiques, leur délai maximum d'interruption, le niveau de service minimum à assurer et les moyens nécessaires pour le faire.
De ces besoins nait la stratégie de continuité, qui guide la mise en place des mesures, essentiellement matérialisées par des systèmes, procédures et modes opératoires adaptés, coordonnés entre eux et appuyés sur des moyens déployés. Le PCA est donc un plan d'action écrit, complet et détaillé à mettre en œuvre en cas de perturbation.

Le PCA d'une organisation se construit de différentes composantes identifiées, et notamment sa déclinaison en plusieurs PCA métiers, qui couvrent les activités critiques de l'organisation, puis les PCA des fonctions supports qui accompagnent ces PCA métiers en leur fournissant les ressources et moyens qui leur sont nécessaires.
Parmi les composantes essentielles du PCA, on retrouve également le PRA, décliné pour chaque activité critique parallèlement aux PCA métiers et fonctions supports, ainsi que les dispositifs transverses de PSI et de gestion de crise.
Un PSI, ou Plan de Sauvegarde Informatique, est conçu pour gérer le risque de perte des ressources informatiques, essentiellement matérielles, logicielles et de données. Il peut par ailleurs intégrer le système de télécommunications de l'organisation. Il est complémentaire aux PCA métiers, en ceci qu'il contribue à fournir les moyens techniques qui leur sont nécessaires.
La Gestion de Crise prévoit quant à elle les dispositifs d'alerte et de réaction immédiate en cas de survenance d'un évènement. C'est ce qui va notamment déclencher le PCA. Elle pilote par ailleurs le déploiement du PCA lorsqu'il est déclenché et la communication de crise (interne et externe), ainsi que le retour d'expérience après la crise.
Une organisation globale prévoit l'articulation et la coordination de ces composantes entre elles, formalisant notamment les dispositifs organisationnels relatifs à la sécurité et la logistique de crise. Elle prévoit en outre un PRA global pour le retour de l'organisation à une situation normale. Réunies, toutes ces composantes forment le PCA de l'organisation.

Cette définition générique du PCA est applicable à toute organisation, indépendamment de sa nature, de sa taille, ou de son secteur d'activité. La différenciation se manifestera dans sa conception détaillée, au travers de risques majeurs et activités critiques spécifiques, et des particularités des enjeux du secteur. Par ailleurs, la règlementation relative au PCA peut également présenter des spécificités selon le secteur d'activité considéré.

1.2 Règlementation et normes

La prise de conscience progressive des sociétés autour de l'importance fondamentale de la continuité d'activité dans les organisations pour atténuer les effets des incidents perturbateurs amène aujourd'hui le législateur et les régulateurs à se positionner sur le sujet.
Ainsi, une législation naissante vient poser un certain nombre d'exigences de continuité d'activité, en particulier pour les acteurs économiques fournissant un service publique. Cela fournit l'assurance que ces acteurs sont dotés de dispositifs appropriés pour garantir la continuité des activités.
Parallèlement, un référentiel normatif balise peu à peu le sujet et guide les organisations désireuses de le faire, dans la mise en place de leur continuité d'activité.

1.2.1 Référentiel normatif générique

La norme ISO 22301 (Sécurité Sociétale – Systèmes de Gestion de la Continuité des Activités – Exigences), parue en 2012, se pose comme le standard international de management de la continuité.
Un référentiel reconnu des bonnes pratiques en gestion de continuité des activités était nécessaire, notamment à des fins de certification. Plusieurs pays avaient déjà soulevé cette problématique, et notamment le Royaume-Uni avec la norme britannique BS 25999 (British Standard : organisme de normalisation au Royaume-Uni, équivalent de l'AFNOR en France) qui avait pour objet d'aider à mettre en place un système de gestion de la continuité d'activité, et était la première du genre.
La norme ISO 22301 vise à remplacer ce standard britannique, et a été élaborée en coopération et avec des contributions du monde entier. Elle a été développée pour permettre aux organisations de minimiser l'impact de sinistres majeurs.
Cette norme spécifie formellement un ensemble d'exigences pour mettre en place et maintenir, dans une logique d'amélioration continue, un dispositif de continuité d'activité, menant à une certification.
Les exigences spécifiées dans la norme sont génériques et prévues pour s'appliquer à toute organisation ou partie de celle-ci, indépendamment du type, de la taille et de la nature de l'organisation. Elle met notamment en exergue l'importance de comprendre les besoins de l'organisation et la nécessité de définir une politique et des objectifs de continuité, de déployer et mettre en œuvre les moyens nécessaires pour les atteindre et de surveiller et revoir le dispositif afin d'en assurer l'amélioration continue.
Dans le cas particulier de la continuité d'activité informatique et la mise en place d'un PSI, un référentiel normatif spécifique existe, ainsi que des bonnes pratiques internationales. En particulier, la norme britannique BS 25777 guide l'établissement d'un cadre organisationnel du PSI. Le British Standard propose également un recueil de bonnes pratiques pour réaliser les tests du PSI, notamment sur le data center. Cette norme a inspiré l'ISO pour créer la norme 27031 portant sur la continuité informatique.
L'intérêt pour une organisation de se conformer au référentiel proposé par la norme ISO 22301 pour mettre en place un PCA et la norme ISO 27031 pour en définir le PSI, au-delà de la guidance que cela fournit, est que cette certification prouve son respect des bonnes pratiques en la matière auprès des instances législatives et règlementaires, des clients potentiels et d'autres parties prenantes intéressées.

En effet, conscients de leur interdépendance, les acteurs cherchent à s'assurer que leurs principaux fournisseurs et partenaires sont toujours en mesure de pouvoir fournir les produits et services critiques, même en cas d'incidents. Cette exigence peut être imposée par leur propre PCA. Certains actionnaires, soucieux de protéger leur fonds, peuvent également être sensibles à ce type de certifications. Enfin, certaines primes d'assurance diminuent pour l'entreprise à risque si elle est dotée d'un PCA certifié.

1.2.2 Cadre législatif et règlementaire spécifique

Les PCA sont obligatoires et règlementés dans certains secteurs d'activités, notamment les fournisseurs de services vitaux : Banques et assurances, santé publique, alimentation, énergie, transports, et télécommunications. Les secteurs d'activités d'importance vitale, ainsi que toutes les dispositions qui s'y rapportent, sont définies dans les articles R. 1332-2 et suivants du Code de la Défense. Une base de données unique tenue et mise à jour par le secrétariat général de la défense nationale rassemble l'ensemble des informations spécifiques du dispositif de sécurité des activités d'importance vitale. Elle porte le nom de « DIVA » (Données d'Importance Vitales).

1.2.2.1 Secteurs bancaire et assurantiel

Les secteurs banque et assurance sont particulièrement encadrés en Europe en ce qui concerne la continuité d'activité.
Le règlement CRBF 97-02 traite de la problématique des PCA pour le secteur bancaire. Bien que la thématique soit abordée de manière assez succincte, la définition du PCA est formalisée par l'article 4, et les exigences minimales de continuité sont fixées par les articles 14, 37, 39 et 40. Ainsi il est imposé aux établissements financiers de définir et maintenir un niveau de sécurité informatique adéquat, y adapter leurs SI et prévoir des procédures afin d'assurer la continuité d'exploitation en cas de difficultés graves. Au-delà de la continuité informatique, ils doivent disposer d'un PCA complet, et prévoir la continuité des activités externalisées ou sous-traitées.
Par ailleurs, les éléments de contrôle interne, et en particulier ceux relatifs à la continuité d'activité et la continuité informatique, doivent être formalisés via des manuels de procédures et faire l'objet d'une revue régulière par l'organe délibérant, sur la base des informations transmises par l'organe exécutif.
A l'intérieur de ce cadre réglementaire, les établissements disposent d'une certaine marge de manœuvre sur la façon dont les PCA sont mis en place pour répondre à ces exigences.
Dans le secteur de l'assurance et la réassurance, le texte Solvency II évoque la nécessité pour les établissements de prendre des mesures raisonnables afin de veiller à la continuité de leurs activités, dans l'article 4.

Le secteur bancaire est très règlementé, et à juste titre. L'activité bancaire est un secteur critique et vital pour le fonctionnement de l'économie. Il est donc très surveillé au niveau national, mais aussi international, du fait des interdépendances entre les nations ainsi que pour le maintien de la stabilité des marchés financiers.

On identifie trois grands acteurs de la régulation dans le bancaire :

L'ACP : Autorité de Contrôle Prudentiel

Anciennement la commission bancaire, l'ACP est l'organe de contrôle de la banque de France. Son rôle est fixé par l'article L613-1 du code monétaire et financier :
« La commission bancaire est chargée de contrôler le respect par les établissements de crédit des dispositions législatives et réglementaires qui leur sont applicables et de sanctionner les manquements constatés.
Elle examine les conditions de leur exploitation et veille à la qualité de leur situation financière.
Elle veille au respect des règles de bonne conduite de la profession. Elle veille également à ce que les entreprises soumises à son contrôle mettent en œuvre les moyens adaptés pour se conformer aux codes de conduite homologués mentionnés à l'article L. 611-3-1.
Elle propose et demande la mise en œuvre du fonds de garantie des dépôts dans les conditions prévues par les articles L. 312-5 et L. 613-34. »

AMF : L'Autorité des Marchés Financiers

L'AMF veille quant à elle à la protection des épargnants dans le cadre des appels publics à l'épargne ou d'introduction d'instruments financiers sur les marchés, à la fiabilité de l'information fournie aux acteurs des marchés financiers et au bon fonctionnement des marchés.

Comités de Bâle

A ces organismes de régulation français, viennent s'ajouter les règlementations émanant des comités internationaux de Bâle (1, 2 et 3) sur le contrôle bancaire, en anglais Basel Committee on Banking Supervision.
Ce comité a lieu 4 fois par ans, et y sont traités tous les sujets liés à la supervision bancaire. Il se compose des représentants des banques centrales et des autorités prudentielles de treize pays : Etats-Unis, Allemagne, France, Suisse, Japon, Canada, Espagne, Italie, Luxembourg, Pays-Bas, Royaume-Uni, et Suède.
Ses missions sont, entre autres, de veiller au renforcement de la sécurité et de la fiabilité du système financier, d'établir des standards en matière de contrôle prudentiel, et de promouvoir une coopération internationale sur ces sujets.

1.2.2.2 Secteur de la santé publique

Le législateur a défini un cadre règlementaire régissant la gestion de crise et la continuité d'activité des établissements de santé, dont le fondement est donné par la loi du 9 Août 2004 relative à la politique de santé publique. Ainsi, tout établissement de santé est dans l'obligation règlementaire de disposer d'un plan lui permettant de mobiliser immédiatement les moyens dont il dispose pour faire face à une situation d'urgence sanitaire, qu'il appartienne ou participe au service public hospitalier comme au secteur privé. Cette loi est complétée par le décret du 30 Décembre 2005 et la circulaire n° DHOS/CGR/2006/401 du 14 Septembre 2006. Ces textes imposent aux établissements de santé disposant d'un service d'urgences, la mise en place de dispositifs de gestion de crise, incluant la prévention et la gestion des crises en interne, un dispositif d'urgence appelé "plan blanc" en interne,

ainsi que l'intégration de chaque établissement dans le "plan blanc élargi" de son département d'appartenance, déclenché par le préfet en cas de crise.
En effet, de par leur rôle sanitaire et social, les établissements de santé doivent être en mesure de faire face à la fois à un éventuel sinistre interne, mais également de fournir un support aux crises sanitaires et sociales entrainant un afflux de victimes. Une coordination de l'ensemble du système de santé est prévue pour parer à ces crises, dans laquelle chaque établissement doit être apte à s'intégrer.
A la circulaire du 14 Septembre 2006 est annexé un guide d'aide à l'élaboration des plans blancs élargis et des plans blancs des établissements de santé. En outre, des serveurs régionaux visent à collecter des informations régulièrement sur la situation des établissements de santé de sa juridiction, assurant ainsi une veille de prévention de crise globalisée.
Par ailleurs, des établissements de santé référents sont identifiés par le décret du 30 Décembre 2005, dont la mission principale est de fournir une assistance aux autres établissements de santé dans le cadre du déclenchement d'un plan blanc élargi.

1.2.2.3 Secteur Alimentaire

Il existe une pléthore de lois encadrant l'industrie agroalimentaire, et ce dans un souci de santé publique et de protection des consommateurs.
Lorsqu'on parle des PCA ou du dispositif de gestion de crise, il convient tout d'abord d'adopter le point de vue de l'organisation et de réfléchir aux crises qui pourraient porter préjudice à la continuité de l'activité, et ensuite d'en déduire les normes et règles auxquelles l'entreprise doit se soumettre dans l'éventualité où ce genre de scénario se réaliserait.

Il existe par conséquent un cadre législatif et normatif anticipant les situations de crises alimentaires et permettant de les réguler ou de limiter leurs impacts.

Cadre législatif

En règle générale, on identifie deux grandes sources de législation émanant du gouvernement Français et de l'Union Européenne concernant la sécurité alimentaire :

Il y a en premier lieu la Direction Générale de l'Alimentation, qui met à disposition des professionnels de l'agroalimentaire toute la législation les concernant :

- Santé et protection des animaux d'élevage et domestique, pharmacie vétérinaire, identification et mouvement des animaux, alimentation animale, sous-produits,…
- Santé et protection des végétaux
- Prévention des pollutions, agriculture raisonnée
- Sécurité sanitaire des aliments, nutrition
- Organismes Génétiquement Modifiés, signes d'identification de la qualité et de l'origine, etc...

On identifie d'autre part le Règlement (CE) n°178/2002 du Parlement européen et du Conseil du 28 Janvier 2002, établissant les principes généraux et les prescriptions générales de la législation

alimentaire, instituant l'Autorité Européenne de Sécurité des Aliments et fixant des procédures relatives à la sécurité des denrées alimentaires.

Plus concrètement, au niveau de la gestion de crise, la Direction Générale de la Consommation (Ministère des Finances) a mis en place un guide d'aide à la gestion des alertes d'origines alimentaires. Il s'agit d'un guide qui a pour but de mettre en place des actions rapides, concertées et efficaces dans le cas d'une situation d'alerte sanitaire.

L'HACCP : Hazard Analysis Critical Control Point

L'HACCP est un système d'analyse des dangers et des points critiques pour leur maitrise. Cette méthode de maîtrise de la sécurité sanitaire des denrées alimentaires a été mise au point aux Etats-Unis par un laboratoire de la NASA. L'objectif était la prévention, la réduction ou l'élimination de tout danger biologique, chimique ou physique autour des denrées alimentaires.
C'est aujourd'hui un référentiel standard imposé par différentes autorités européennes (notamment par le règlement n°178/2002 du Parlement Européen) pour l'hygiène des aliments. Il a été introduit dans l'Union Européenne en 1993 par la directive n°93/43/CE relative à l'hygiène des denrées alimentaires.

Cette méthode repose sur sept grands principes :

Principe 1 : Procéder à une analyse des dangers
Principe 2 : Déterminer les points critiques pour en assurer la maîtrise
Principe 3 : Fixer les seuils critiques
Principe 4 : Mettre en place un système de surveillance des mesures de maîtrise aux dangers identifiés
Principe 5 : Déterminer les actions correctives à mettre en œuvre lorsque la surveillance révèle qu'une mesure de maîtrise à un CCP donné est défaillante
Principe 6 : Appliquer des procédures de vérification afin de confirmer que le système HACCP fonctionne efficacement
Principe 7 : Constituer un dossier dans lequel figurent toutes les procédures et tous les relevés concernant ces principes et leur mise en application (traçabilité)

Cette méthode est notamment très efficace pour réguler les dangers de contamination des aliments, qui constituent un risque critique dans l'industrie agroalimentaire.

Norme 22000

A ce cadre législatif s'ajoute la norme internationale relative à la sécurité des denrées alimentaires, l'ISO 22000. Elle traite d'une part le risque sanitaire que peut présenter une crise alimentaire pour les consommateurs, mais aussi la gestion de crise en général dans l'industrie agroalimentaire et des risques critiques pour ce secteur particulier.
Toutes ces recommandations de l'AFNOR entrent bien sûr en ligne de compte dans la stratégie de management de la crise et du PCA. Ces deux volets de la gestion du risque sont obligatoires puisque l'alimentaire fait partie des activités dites vitales et doit de fait assurer la continuité de ses activités.

1.2.2.4 Secteur de l'Energie

Règlementation SAIV des Opérateurs d'Importance Vitale

Comme tous les Opérateurs d'Importance Vitale (OIV : dont la liste des secteurs désignés comme tel a été fixée le 2 Juin 2006 par arrêté ministériel), le secteur de l'énergie (électricité, gaz, pétrole, nucléaire civil) et plus particulièrement ici, la distribution du gaz, est règlementé et contrôlé principalement par le Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN).
Ce statut particulier, qui concerne la majorité des secteurs que nous avons choisi d'étudier, les oblige à assurer la continuité de leurs activités en toutes circonstances, car tout comme dans le bancaire ou la santé par exemple, l'arrêt de l'activité, en l'occurrence de la distribution du gaz, et ce même pendant quelques heures, aurait des conséquences dramatiques à de multiples niveaux. En effet, la plupart organisations dépendent de leur alimentation en énergie et donc de la fiabilité des opérateurs qui en assurent la distribution.Le SGDSN met par ailleurs à la disposition de ces activités un guide complet de mise en place des plans de continuité et de la gestion de crise.

Instances de contrôle : Commission Interministérielle de Défense et de Sécurité

Au-delà des mesures prises en interne (audits, contrôles de conformité, etc.), des contrôles portant sur la sécurité et la continuité des plans peuvent avoir lieu de façon ponctuelle ou sur demande d'un ministre coordinateur par la commission interministérielle de défense et de sécurité.

Ministère de l'Economie et du Développement Durable

Ce ministère est l'autorité de tutelle d'un point de vue technique sur le secteur. Il est systématiquement informé des sinistres d'une certaine importance (exemple : 10 000 personne dont l'alimentation en gaz est coupée), et effectue des contrôles réguliers.

1.2.2.5 Secteur des Transports

L'essentiel de la règlementation relative au transport public est issu du Code des Transports (Version consolidée au 18 Juillet 2013), et en particulier de l'ordonnance n°2010-1307 du 28 Octobre 2010 relative à la partie législative du code des transports.
Ces textes définissent le transport public comme tout transport de personnes ou de marchandises, à l'exception de celui organisé pour son propre compte par une personne, publique ou privée, et de ceux relevant d'une autre réglementation. Cela concerne le transport ferroviaire, le transport routier, la navigation intérieure et le transport fluvial, le transport et la navigation maritimes, ainsi que l'aviation civile. Les missions de service public consistent notamment en la réalisation et la gestion d'infrastructures et d'équipements affectés au transport et leur mise à la disposition des usagers, l'organisation du transport public, la réglementation des activités de transport et le contrôle de son application, et le développement de l'information sur les transports.
En cas de perturbation prévisible du trafic (grèves, travaux, incidents techniques, aléas climatiques ou tout autre évènement connu dans un délai de 36 heures), l'organisation chargée des transports se doit d'assurer les dessertes prioritaires, et détermine le niveau de service minimum en fonction de

l'importance de la perturbation. Elle doit par ailleurs tenir le représentant de l'Etat et les autorités compétentes informées.
Le niveau de service minimum doit permettre d'éviter que soit portée une atteinte disproportionnée à la liberté d'aller et venir, à la liberté d'accès aux services publics, à la liberté du travail, à la liberté du commerce et de l'industrie et à l'organisation des transports scolaires. Il correspond à la couverture des besoins essentiels de la population. Il doit également garantir l'accès au service public de l'enseignement les jours d'examens nationaux. Il prend en compte les besoins particuliers des personnes à mobilité réduite.
Lors de perturbations du trafic, tout usager a le droit de disposer d'une information gratuite, précise et fiable sur le service assuré, au plus tard vingt-quatre heures avant le début de la perturbation.
Après chaque perturbation, un bilan détaillé de l'exécution du plan de transports adapté et du plan d'information des usagers doit être formalisé, de même qu'une évaluation annuelle des incidences financières de l'exécution de ces plans et la liste des investissements nécessaires à l'amélioration de leur mise en œuvre. Cette évaluation est rendue publique.
D'une manière générale, l'ensemble des incidents doit être notifié au représentant de l'Etat et aux instances de tutelle, conformément à la directive européenne n°2003-42 du 13 Juin 2003 relative aux comptes rendus d'événements dans l'aviation civile, transposée en droit français. Dans le cas d'un incident grave, celui-ci doit être notifié directement au BEA (Bureau d'Analyse et d'Enquête pour la Sécurité de l'Aviation Civile). Les arrêtés du 4 Avril 2003 et du 17 Août 2007 fixent la liste des évènements et incidents d'aviation civile devant être rapportés.
En complément de ces dispositions, la loi n°2012-375 du 19 Mars 2012 relative à l'organisation du service et à l'information des passagers dans les entreprises de transport aérien de passagers et à diverses dispositions dans le domaine des transports (également connue comme la loi Diard), précise les éléments relatifs à l'exercice du droit de grève du personnel des transports.
Ces obligations règlementaires sont complétées par des engagements pris auprès du CGEDD (Conseil Général de l'Environnement et du Développement Durable) relatifs à la viabilité hivernale suite aux épisodes neigeux de Décembre 2010 (14 Novembre 2011). Parmi les entreprises concernées par ces engagements, on retrouve la RATP (Régie Autonome des Transports Parisiens), la SNCF (Société Nationale des Chemins de Fer), les ADP (Aéroports De Paris), le RFF (Réseau Ferré de France).
En outre, des instances de tutelle existent, relatives aux différents types de transport, notamment l'Autorité de Régulation des Activités Ferroviaires, l'OACI (Organisation de l'Aviation Civile Internationale) ou la DGAC (Direction Générale de l'Aviation Civile).

1.2.2.6 Secteur des Télécommunications

A l'origine de la règlementation sur le secteur des télécommunications, on trouve des directives européennes, notamment 4 directives du 7 Mars 2002 (directives "cadre", "autorisations", "accès" et "service universel") et directives des 12 Juillet 2002 (données personnelles) et 16 Septembre 2002 (concurrence). Ces directives ont été transposées en droit national par trois lois, celle du 31 Décembre 2003 relative aux obligations de service public des télécommunications et à France Télécom (service universel), celle du 21 Juin 2004 pour la confiance dans l'économie numérique, et celle du 9 Juillet 2004 relative aux communications électroniques et aux services de communications audiovisuelles. Les dispositions de ces trois lois ont été codifiées dans le Code des Postes et des Communications Electroniques (CPCE). Elles définissent les obligations de service public du secteur des télécommunications, et notamment le service universel, détaillé ci-après.

Les opérateurs du secteur des télécommunications sont régulés par l'autorité de tutelle qu'est l'ARCEP (Autorité de Régulation des Communications Electroniques et des Postes), qui a notamment la faculté de fixer, dans le cadre de la loi, des obligations générales qui s'appliquent à tous les opérateurs. Elle dispose en outre d'un pouvoir de sanction à l'égard des opérateurs qui ne respectent pas leurs obligations.

Service universel

La notion de service universel est imposée aux opérateurs de télécommunications par la loi du 31 Décembre 2003 relative aux obligations de service public des télécommunications et à France Telecom. L'objectif du service universel est de fournir un ensemble minimal de services déterminés à tous les utilisateurs finals à un prix abordable.
Le service universel est l'une des trois composantes du service public en matière de télécommunications, avec la fourniture de services complémentaires (anciennement dits obligatoires) de communications électroniques et des missions d'intérêt général.
Les prestations de service universel sont assurées sur l'ensemble du territoire et se composent de trois dimensions :

- Le service téléphonique (installation et opération, pour toute personne le demandant, d'un raccordement fixe au réseau ouvert au public, et fourniture d'un service téléphonique de qualité à un tarif abordable)
- L'annuaire universel et le service universel de renseignements (service de renseignements et distribution gratuite d'un annuaire imprimé à tout abonné au service de téléphonie public)
- La publiphonie (installation et entretien de cabines téléphoniques sur le domaine public, et fourniture, dans ces cabines, d'un service téléphonique de qualité à un tarif abordable)

Pour chacune de ces composantes, des dispositions spécifiques sont prises en faveur des personnes handicapées, dans la limite des technologies disponibles pouvant être mises en œuvre à un coût raisonnable.
La tarification des services est par ailleurs encadrée.

Le secteur d'activité des télécommunications appartient aux secteurs d'importance vitale, et est donc régi par la circulaire n°6600/SGDSN/PSE/PPS du 26 Septembre 2008 relative à la sécurité des activités d'importance vitale (SAIV). Cette circulaire impose aux opérateurs du secteur la mise en place de plans de sécurité et de continuité d'activité, afin de garantir la continuité des services publics dont ils sont responsables.

1.2.2.7 Crises sanitaires et pandémies grippales

Dans le cadre des crises sanitaires, et notamment des pandémies grippales, de nombreux gouvernements ont menés des études afin d'estimer l'impact d'une telle pandémie sur l'économie. Ainsi, les fournisseurs de services vitaux ont été invités à intégrer cette dimension dans leur PCA, de manière à pouvoir fournir un service minimum malgré un manque de personnel.

Un PCA va au-delà du simple respect des règles et normes, il n'est pas à envisager seulement sous l'angle de la conformité. Il faut s'interroger plus globalement sur le maintien des activités critiques.

1.3 La mise en place d'un PCA : Référentiel générique des bonnes pratiques

Se doter D'un PCA incluant un PRA correspondant, un PSI et une gestion de crise est un enjeu majeur pour les organisations. Celui-ci doit être conçu, documenté et déployé préalablement à la survenance d'une crise pour qu'il trouve son utilité. La conception et le déploiement d'un PCA s'inscrivent dans le cadre d'un projet PCA qui s'étale sur plusieurs années et mobilise l'ensemble de l'organisation. Le PCA doit ensuite être maintenu en condition opérationnelle et mis à jour régulièrement.

1.3.1 La conception du PCA

Préalable

- **Communication Interne**

Etape 1

- **Constitution de l'équipe chargée de la mise en place du PCA**

Etape 2

- **Définir les activités critiques et la stratégie de continuité**
- Phase 1 => Identification des activités critiques
- Phase 2 => Elaboration de la stratégie de continuité
- Phase 3 => Validation de l'étape

Etape 3

- **Etudier et choisir les solutions envisageables**
- Phase 1 => Etude de faisabilité et chiffrage des solutions
- Phase 2 => Evaluer la pertinence des solutions
- Phase 3 => Prise de décision : Choix des solutions

Etape 4

- **Mettre en place une base documentaire**
- Base documentaire
- Les livrables PCA incontournables

Etape 5

- **Prévoir une politique de communication**
- Communication Interne
- Communication Externe
- Problématiques de confidentialité

Préalable

Un PCA impose une action spécifique de communication en interne visant à sensibiliser l'organisation à la gestion du risque, à la continuité d'activité, et à préparer la conduite du changement. Cette communication interne est un préalable nécessaire à toute démarche de continuité d'activité.

1.3.1.1 Constitution de l'équipe en charge de la mise en place du PCA

La mise en place d'un PCA est un acte de gouvernance d'entreprise et mobilise l'ensemble du personnel de l'organisation. Le projet s'appuie fortement sur la Direction Générale, les instances de pilotage du projet et les différents acteurs de la démarche.

a) Les organes de gouvernance du PCA

L'organisation générale du projet est surveillée et soutenue par les organes de pilotage du PCA. L'essentiel des prises de décisions leur incombe, avec une validation de toutes les étapes de construction du PCA par la DG.

Le comité de pilotage

Cet organe a un caractère décisionnel et de pilotage.
Il est présidé par le commanditaire du PCA, généralement la Direction Générale, ou un représentant de celui-ci, et co-animé par le RPCA et le RPSI. Les responsables des principales fonctions support y participent éventuellement, accompagnés des responsables des métiers critiques. Les fonctions en charge de la gestion des risques et des contrôles (Management des Risques, Contrôle Interne, Conformité, Contrôle Permanent) doivent être associées à la démarche. La présence de l'Audit Interne peut être envisagée à titre informatif et non décisionnel, mais il faut veiller à ce que cette présence ne soit pas interprétée comme une validation des décisions au fil de l'eau.
La composition du comité de pilotage, ses pouvoirs et sa périodicité sont formalisés. Il est recommandé qu'il se réunisse entre 1 et 4 fois par an et prenne l'ensemble des décisions relatives au projet PCA, aux différentes étapes successives. Il est destinataire du reporting PCA. Les ordres du jour et comptes-rendus des réunions sont formalisés et communiqués à l'Audit Interne.

Le comité opérationnel

Cet organe assure le pilotage opérationnel du projet PCA. Il est présidé par le RPCA (Responsable PCA) et se compose des CCA (Correspondants Continuité d'Activité) métiers et fonctions supports et du RPSI (Responsable PSI).
Il a pour rôle de piloter le processus de continuité d'activité et de préconiser des améliorations. Il centralise également le reporting PCA avant sa transmission au comité de pilotage. Sa composition, ses pouvoirs et sa périodicité sont documentés, et ses ordres du jour et comptes-rendus formalisés.

b) Le Responsable du Plan de Continuité d'activité (RPCA)

Le RPCA est un acteur clé de la démarche PCA, il porte le projet et rassemble et coordonne les différents acteurs. Il doit avoir une autorité reconnue dans l'organisation, le soutient de la Direction Générale et un rattachement hiérarchique approprié, de manière à être légitime pour animer la démarche et pouvoir influer sur les décisions avec une supervision d'ensemble.
Il doit être indépendant de toute fonction opérationnelle, en particulier de l'informatique ou des Moyens Généraux qui n'ont pas une vision « métier » de l'organisation. Idéalement le RPCA devrait être totalement dédié à cette fonction, mais en fonction des organisations, cela n'est pas toujours possible. Il ne doit cependant pas relever de l'Audit Interne.
Il est important que le RCPA soit doté d'un bon sens de l'organisation et de la capacité à animer un réseau et communiquer. Il doit également disposer d'un bon niveau de connaissance et de compréhension des exigences normatives et règlementaires, des SI et des techniques et référentiels de Management des Risques et de Contrôle Interne.
Puisqu'il anime la continuité d'activité, il doit être reconnu en interne et en externe comme un interlocuteur légitime et incontournable sur le sujet, et être en mesure de mobiliser les ressources et moyens nécessaires à la mise en œuvre de la continuité d'activité, tant lors du projet que du maintien en condition opérationnelle.
Le RPCA travaille en constante synergie avec tous les acteurs du PCA, à travers la participation aux comités liés. Par ailleurs, il peut participer aux comités de sécurité et des risques de l'organisation pour garantir l'homogénéité des démarches liées aux risques.
Le rôle du RPCA, formalisé dans une fiche de poste et/ou une lettre de mission, comporte plusieurs volets.
Tout d'abord, il anime le projet PCA, à travers notamment le réseau CCA (Correspondants Continuité d'Activité) et RPSI qu'il doit sensibiliser, informer, former, accompagner, et à qui il doit fournir les outils nécessaires. Il met en place une organisation de projet qu'il pilote, en gérant notamment les moyens et ressources allouées.
Il se fait l'intermédiaire entre les métiers, fonctions supports et la Direction Générale, s'assurant que les besoins de chacun sont pris en compte dans le PCA (notamment les directives de la Direction Générale) garantissant la circulation de l'information et des reportings. Il fait également le lien avec la gestion de crise et des incidents.
Il est responsable de la conception de l'organisation globale qui coordonne les différents aspects qui composent le PCA, ainsi que la mise en place de la gestion de crise et des incidents. Il se charge également d'organiser le déploiement et les tests du PCA, ainsi que son maintien en condition opérationnelle, et de communiquer sur ces sujets. Il intègre la continuité d'activité au quotidien, et s'assure de son amélioration continue (veille à l'application des recommandations des audits, retours d'expérience et demandes de la Direction Générale).
Par ailleurs, le RPCA a un rôle important vis-à-vis des acteurs externes. Il peut notamment être un porte-parole de l'organisation dans le cadre de la politique de communication, ou faire le relais avec le service communication.
Il assure une veille et garantit la conformité du PCA vis-à-vis des instances de tutelle, des régulateurs, du Conseil d'Administration ou de toute instance de surveillance. Il assure donc la remontée des informations vers les parties prenantes.

Il représente l'entreprise auprès des associations professionnelles et des organismes spécialisés, et il est également impliqué dans la négociation de tous les aspects contractuels relatifs à la continuité d'activité (sites de repli, outils, logiciels, prestataires de secours…).
Enfin le RPCA assure un rôle spécifique lors de la survenance d'une crise, où il se positionne en appui transverse. Il pilote la gestion de la crise, participe activement au diagnostic en cas d'alerte, conseille la Direction Générale et aide les acteurs (CCA) dans leur mise en place de la continuité d'activité.
Compte tenu de l'importance du RPCA dans la démarche de continuité d'activité, cet acteur doit être identifié dès le démarrage du projet, et la personne, ses fonctions et responsabilités, son rôle, doivent être clairement formalisées.
Il doit par ailleurs disposer d'un suppléant afin d'assurer la permanence du poste.

c) Le responsable du plan de secours informatique (RPSI)

Le RPSI est le pilote du PSI. Il est plus souvent rattaché à la DSI car les enjeux et les considérations techniques y sont localisés.
Il est essentiel d'identifier un RPSI. En effet en l'absence de responsable spécifique de la continuité informatique, il existe une forte probabilité pour que le sujet ne soit pas traité correctement. Il vaut mieux que le RPSI soit différencié du DSI, qui gère déjà une activité au quotidien et peut difficilement s'occuper également des cas de sinistre.
Le PSI visant à fournir un support aux PCA métier, il va chercher à répondre aux besoins exprimés par les opérationnels. Dans un domaine technique, où opérationnels et informaticiens ne parlent pas forcément le même langage, le RPSI devra s'assurer de la compréhension, la collaboration et la coordination entre les différentes parties prenantes liées aux PSI.
Il va également superviser la réalisation technique et les tests du PSI, ainsi que prendre les décisions s'y afférant, en fonction des délégations de pouvoirs en vigueur dans l'organisation (recours à des prestataires externes par exemple). Il gère le budget du PSI et s'assure que celui-ci répond aux objectifs fixés par la DG et dans la stratégie de la continuité. Il est membre à part entière du réseau RPCA, et veille à l'intégration du PSI dans le PCA global de l'organisation.

d) Les correspondants continuité d'activité (CCA).

Ils sont le relais du RPCA dans toute l'organisation. Installés dès le début du projet PCA par le RPCA avec la validation du comité de pilotage PCA, leur rôle perdure pendant toute la durée de vie du PCA, à travers la conception, le déploiement et la maintenance du PCA. Il s'agit de responsables PCA métiers, chacun en charge d'une activité critique (propriétaires de processus), ainsi que du RPSI et des responsables de la continuité des processus supports (Ressources Humaines, Communication, Moyens Généraux, Achats, Administration et Finances…).
De la même manière que le RPCA, leur désignation, fonctions et responsabilités, rôle, sont définis et formalisés dans des fiches de poste. Cette formalisation est d'autant plus nécessaire lorsque les personnes désignées occupent d'autres fonctions.

e) Engagement de la direction

L'engagement de la Direction Générale est capital dans une démarche PCA. En effet, il s'agit d'une thématique qui mobilise l'ensemble de l'organisation, avec des impacts multiples.

Fortement appuyée sur le RPCA et son réseau, la gouvernance doit néanmoins avoir une implication perceptible pour intégrer la continuité d'activité dans la culture de l'organisation. C'est notamment sur elle que repose la désignation des membres des comités opérationnel et de pilotage du PCA, celle du RPCA et RPSI.
L'engagement de la direction peut être formalisé dans une lettre d'engagement.
La Direction Générale est également l'interlocuteur du Conseil d'Administration sur la problématique des PCA, avec l'appui éventuel du RPCA, et doit l'informer de la démarche et recueillir ses attentes sur le sujet.

1.3.1.2 Définir les activités critiques et la stratégie de continuité

Cette définition constitue la première étape de la conception du PCA. En effet, la mise en place de la continuité d'activité d'une organisation s'appuie sur la connaissance des processus, des activités, des risques et des ressources de celle-ci. C'est cette connaissance approfondie qui va permettre d'identifier les activités critiques et de définir la stratégie de continuité, qui guidera ensuite l'ensemble de la démarche PCA. Cette étape est critique, c'est d'elle dont dépend la pertinence du projet.

a) <u>Phase 1 : Identification des activités critiques</u>

Il convient tout d'abord de définir ce que sont les activités critiques. Il s'agit donc des activités dont l'interruption aurait des conséquences graves pour l'organisation, tant opérationnelles que financières, juridiques ou d'image.
La démarche d'identification des activités critiques d'une organisation suit une méthodologie jalonnée d'étapes.

Cartographie des processus

Dans un premier temps, il est nécessaire de recenser tous les processus de l'organisation, qu'ils concernent les métiers, les fonctions support ou la gouvernance. Cela s'accompagne de l'inventaire complet des ressources et moyens qui leur sont nécessaires, ainsi que de leurs contributions respectives aux résultats financiers.

Cartographie des risques

Parallèlement, une cartographie des risques doit être élaborée. Elle couvrira l'ensemble des risques, majeurs ou non, et à la fois ceux qui portent sur l'ensemble de l'organisation et ceux associés à chacun des processus précédemment inventoriés.
Ce recensement des risques peut s'appuyer sur des réflexions menées précédemment sur la problématique des risques, en particulier le Management des Risques, le Contrôle Interne et l'Audit Interne.
Il est par ailleurs intéressant d'associer aux risques identifiés un degré de probabilité d'occurrence, en tenant compte du contexte.

Analyse des impacts d'une interruption d'activité

Pour chacun des processus métiers et l'informatique, au vu des risques qui leur sont associés, le but est d'identifier l'ensemble des conséquences qui découleraient d'une interruption d'activité, en s'attachant à rester objectif, et tout en mobilisant une forte expertise. L'objectivité est particulièrement importante car il existe le risque qu'un responsable de processus qui comprend que son activité n'est pas critique n'ose pas le dire.
Les impacts sont à considérer à la fois sur l'organisation elle-même et sur les différentes parties prenantes qui lui sont liées :

L'impact doit être identifié et mesuré quantitativement et qualitativement, et peut être financier (coût d'une interruption), règlementaire, d'image, d'insatisfaction client, d'inquiétude des collaborateurs et autres parties prenantes…
Cette analyse s'appuie sur des outils et des méthodes. Il convient notamment d'appréhender pour chaque processus ce qui est fait au quotidien et pour quel résultat et quels destinataires (internes et externes), avec la description des flux entrants et sortants. Une analyse des incidents passés et le calcul de la part de marge et de Chiffre d'Affaires impacté sont également des pistes de réflexion.
Cette analyse permet de définir le DMIA (Délai Maximum d'Interruption Acceptable) et le PMDT (Perte Maximale de Données Tolérable), qui sont des éléments essentiels dans la conception d'un PCA.
Le DMIA correspond à la période de temps au bout de laquelle les activités doivent impérativement être restaurées, même en mode dégradé. Le délai de reprise viendra compléter cette information, en précisant le délai avant le retour à une situation normale.
Le PMDT s'exprime en temps de latence entre le dernier état stable à partit duquel une restauration des données est possible et la situation de crise. Concrètement, il s'agit de la fréquence des

sauvegardes et le temps qui s'écoule entre deux sauvegardes, qui constituera le maximum de données qui seront perdues en cas de survenance d'un sinistre.
L'analyse d'impact sera utilisée pour identifier les priorités de reprise et les besoins en continuité, ainsi que les ressources et moyens nécessaires à la reprise d'activité, et servira de fondement à la stratégie de continuité.

Définir la criticité des services en amont et en aval de l'organisation

Dans l'environnement économique actuel où les organisations sont réellement interdépendantes, un sinistre qui toucherait l'une des parties prenantes aurait inévitablement des impacts sur l'organisation considérée. Cette problématique est à évaluer et prendre en compte dans le PCA.
Ces impacts doivent être qualifiés et quantifiés dans la mesure du possible, ce qui n'est pas toujours chose aisée. Ils peuvent être exprimés en fourchette, et concerner les impacts opérationnels et financiers pour l'organisation, puis les répercussions en cascade de l'interruption de ses propres activités due à l'interruption du partenaire.
Cette analyse est à compléter de l'étude des dispositifs de PCA et de maîtrise des risques mis en place par le partenaire.
L'étude relève de la responsabilité des métiers et fonctions supports directement concernés par les partenaires. Ils peuvent éventuellement s'appuyer sur l'expertise d'autres fonctions de l'organisation pour ce faire.

Analyser les dispositifs de maîtrise des risques déjà existants en interne

Les dispositifs mis en place par le Management des Risques et les autres volets du Contrôle Interne de l'organisation viennent réduire les risques qui pèsent sur ces activités et donc en réduire leur criticité. Ils sont donc à prendre en compte dans une démarche d'identification des activités critiques et de mesure de cette criticité.
En particulier, il est intéressant de s'attarder sur les contrats d'assurance souscrits par l'organisation, et qui couvrent une interruption ou une baisse d'activité. Les garanties prévues sont généralement financières, et il faut s'interroger sur le montant et le plafond des indemnités et des éventuelles franchises. On va également s'intéresser aux contrats, notamment aux faits générateurs couverts, aux objets de risques concernés et aux exclusions. Par ailleurs, la fréquence de mise à jour des contrats ainsi que la protection des archives de ceux-ci est également à étudier.

Consulter la Direction Générale

En fonction des objectifs stratégiques de l'organisation et des directives définies par la Direction Générale (et à travers elle par le Conseil d'Administration), certaines activités peuvent s'avérer plus ou moins critiques. Il s'agira ici de prendre en compte ces éléments dans l'identification des activités critiques.
La Direction Générale peut par exemple souhaiter que le PCA permette de garantir le Chiffre d'Affaire, de conserver la confiance des clients et l'image de marque, de tenir les engagements auprès des tiers en cas de crise. Dans le secteur des services publics, le PCA vise plutôt à la sauvegarde de l'intérêt général.

Prendre en compte les obligations règlementaires

Pour certains secteurs d'activité, dits fournisseurs de services vitaux (banques et assurances, santé publique, alimentation, énergie, transports, télécommunications), le législateur et les régulateurs ont défini un niveau de service minimum qui doit être assuré en toutes circonstances. Les activités concernées par ce type de règlementation voient leur niveau de criticité impacté en conséquence.
Cette première phase permet d'identifier les activités critiques et le niveau de cette criticité.

b) Phase 2 : Elaboration de la stratégie de continuité

Ce document est formalisé et approuvé par le comité de pilotage, et fondateur du PCA. Il est incontournable. Il explique les grandes lignes de la continuité d'activité à mettre en œuvre.

Définition des besoins en continuité des métiers

Dans un premier temps, il convient de classer les activités critiques par ordre de criticité, afin de définir les besoins de continuité associés.
Par la suite, et pour chaque activité précédemment identifiée comme critique, le niveau de service ou de production minimum à assurer doit être défini. Cela s'accompagnera de la définition du RPO (Recovery Point Objective) et du RTO (Recovery Time Objective) en cohérence avec le DMIA et le PMDT de chaque activité. Le RTO est le temps dont nous disposons pour mettre en place la solution de secours et revenir à une solution fonctionnelle en mode dégradé. Il est donc logiquement conditionné par le DMIA. Le RPO est connexe et concerne la donnée, il s'agit du point temporel sur lequel il est possible de revenir en matière de données (dernière sauvegarde en date) et est donc fonction du PMDT.
Dans les besoins en continuité, il convient également d'intégrer les délais de reprise, qui prévoient la sortie de crise et le retour à une situation normale.

Imaginer des solutions de PCA métiers

Une fois les besoins en continuité exprimés pour chaque activité critique, des solutions de secours seront imaginées pour y répondre, et assurer la continuité de ces activités en mode dégradé. Les scénarios imaginés devront ramener l'impact d'un choc majeur dans le domaine de l'acceptable.
Il s'agira de s'assurer que les solutions proposées sont à priori faisables (faisabilité technique, organisationnelle et financière), et prévoir l'articulation de ces solutions avec les services support qui peuvent eux aussi être amenés à fonctionner en mode dégradé. Il est également envisageable d'intégrer aux solutions, le recours à des prestataires de secours.
Les PCA doivent prévoir, non seulement d'assurer un service minimum en mode dégradé et garantir ainsi la continuité d'activité, mais également la reprise de l'activité, c'est-à-dire la fin de la situation dégradée, la sortie de crise et le retour à un environnement normal de travail (PRA).
Les solutions doivent intégrer l'identification des acteurs, la définition des rôles et responsabilités, les pouvoirs et délégations de pouvoirs, ainsi que le processus de prise de décision.
Il est important de toujours garder à l'esprit qu'en situation de crise, il s'agit d'évènements imprévus et inattendus, auxquels il faut opposer des solutions différentes et innovantes. C'est en préparant "le pire" que les activités sauront faire face à toutes les situations.

Déterminer les moyens nécessaires aux solutions

Aux solutions formulées vont être associés les moyens et ressources nécessaires à leur déploiement. Il faut commencer par identifier les ressources humaines nécessaires pour déployer la solution et assurer la continuité d'activité et le service minimum en mode dégradé, qui vont être exprimées en termes d'acteurs et de contacts spécifiques.
Il va également falloir déterminer les ressources matérielles qui vont s'avérer indispensables à la solution, incluant le budget alloué, un éventuel site de repli (interne ou externe) et le matériel physique (machines…), ainsi que l'éventuel besoin de recours à des prestataires de secours.
Par ailleurs, il est également capital d'identifier les Systèmes d'Information que mobiliserait le déploiement de la solution, particulièrement en termes d'outils informatiques et bases de données qui doivent être accessibles. Cette première définition des besoins en continuité des SI va permettre de guider l'élaboration du PSI, notamment pour l'évaluation de la criticité des différentes applications et bases de données et donc pour bâtir la stratégie de continuité informatique.
D'une manière générale, les PCA métiers doivent formuler leurs besoins en services supports, pour guider les fonctions support dans l'élaboration de leurs PCA.
Enfin, dans l'éventualité où les ressources disponibles et les moyens de l'entreprise ne correspondent pas aux besoins qui émergent, les solutions devront intégrer des plans d'action pour les rendre disponibles le moment venu.

Définir un PSI (Plan de Secours Informatique)

Le PSI prévoit la continuité des applications informatiques critiques, de l'accès aux bases de données essentielles et des systèmes de télécommunication principaux. Il vise à garantir la fourniture aux activités critiques des moyens SI dont elles ont besoin pour déclencher leurs PCA métiers en cas de survenance d'un sinistre. Il se différencie du PCA métier informatique en ceci qu'il vient en support aux PCA métiers.
Le PSI est à lier avec la sécurité informatique, car certains sujets sont traités en commun. En effet, on parle en sécurité informatique de DICT des systèmes (Disponibilité, Intégrité, Confidentialité, Traçabilité). La "Disponibilité" est le sujet de la continuité informatique.
Préalablement à la conception d'un PSI, il convient de former l'équipe qui sera chargée de sa mise en place, et de mettre au point une organisation et une planification détaillée.

Afin d'élaborer un PSI, la première étape consiste à **identifier les applications et les données qui sont critiques, ainsi que les systèmes sur lesquels elles reposent**, qui sont notamment nécessaires au déclenchement des PCA métiers des activités critiques de l'organisation. C'est sur ces systèmes et applications, et sur l'accès à ces données qu'il est nécessaire d'assurer une continuité de fonctionnement. Dans le cadre d'une organisation qui utilise de très nombreuses applications et bases de données, il n'est pas évident de sélectionner celles qui sont réellement critiques. Par ailleurs, et en fonction des moyens et du budget alloués au PSI, on va chercher à en réduire le nombre, et à justifier les raisons de l'aspect critique.
Idéalement, la sélection se base sur les activités critiques de l'organisation qui ont été identifiées lors de l'élaboration de la stratégie de continuité, et cela permet d'éliminer toutes les applications et bases de données qui n'ont pas trait à ces activités. Ensuite, en fonction du niveau de service minimum défini par les objectifs de continuité de chaque activité critique, cela permet de retirer de

la sélection toutes les applications et bases de données qui ne sont pas indispensables à la fourniture de ce niveau de service minimum.
Lors de l'élaboration des solutions de continuité des PCA métiers, les opérationnels tâchent d'identifier les ressources informatiques qui leur sont nécessaires pour déployer ces PCA. Il reste cependant nécessaire d'affiner ces besoins au travers d'une collaboration étroite entre opérationnels et informaticiens. En effet, ces acteurs n'ont pas le même langage et le même niveau de technicité informatique. Ainsi, ils n'utilisent pas les mêmes appellations pour les applications et bases de données, et les opérationnels n'ont de visibilité que sur l'application ergonomique finale et pas sur l'architecture globale du SI de l'organisation, la façon dont les systèmes s'articulent entre eux et sont interdépendants. Ces difficultés peuvent être contournées via l'établissement de référentiels communs, comme une table de correspondance pour la dénomination des éléments et une cartographie des SI.
Il y a également un travail managérial important afin d'assurer la connexion des acteurs de continuité d'activité et de continuité informatique, et surtout garantir la cohérence entre les deux démarches et leur articulation au sein du PCA global de l'organisation.
Une fois les applications et bases de données critiques identifiées par les opérationnels et les informaticiens, l'engagement que prend le PSI à en assurer la continuité de fonctionnement peut être formalisé via des contrats de service métiers.

La seconde étape de l'élaboration du PSI repose sur **la classification des applications et bases de données critiques en fonction de leur criticité**. Cette classification s'appuie sur une analyse des risques et des impacts qui leur sont liés, ce qui va également permettre d'en justifier la criticité.
L'analyse des risques et des impacts encourus par les applications et bases de données critiques de l'organisation peut se faire en suivant des démarches méthodologiques de type EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) ou MEHARI (Méthode Harmonisée d'Analyse de Risques).
Une évaluation préalable des dispositifs de Contrôle Interne, de sécurité et de continuité déjà existants va s'avérer nécessaire. Le niveau d'obsolescence matérielle et logicielle est également à prendre en compte.
L'identification et l'analyse des risques et des impacts permet de hiérarchiser et de prioriser les éléments de continuité informatique, et de formaliser les besoins, la stratégie et les objectifs de continuité informatique.
Ces éléments sont à faire valider par les instances de pilotage du PCA, ce qui permet d'en valider la conformité aux attentes de la Direction générale.

Cette validation va permettre d'enclencher la troisième étape de mise en place d'un PSI, où **les solutions de secours vont être imaginées**. Ces solutions doivent être cohérentes avec la criticité des applications et bases de données faisant l'objet d'une démarche de continuité, respecter les engagements pris auprès des opérationnels et être conformes à la stratégie de continuité informatique validée. Elles devront intégrer l'ensemble des ramifications du SI et les systèmes sur lesquels reposent les applications et bases de données critiques. Elles devront par ailleurs prévoir la reprise informatique, c'est-à-dire l'accompagnement de la sortie de crise et du mode dégradé vers le retour à un environnement normal de travail. Le premier système à sécuriser est le réseau informatique, base de l'ensemble du SI. Pour les systèmes les plus critiques, des mécanismes de redondances et de doublement du matériel sont à envisager.

Le second élément qu'il est capital de sécuriser, ce sont les données, puisqu'elles constituent un actif extrêmement précieux pour l'entreprise. En fonction de la sensibilité des données, et donc de leur disponibilité, confidentialité et intégrité, celles-ci ne seront pas traitées de la même manière. La criticité des données permet leur classification en deux catégories : Les données importantes, dont il faut assurer la sauvegarde et les données critiques, pour lesquelles il faut prévoir non seulement la sauvegarde, mais également la continuité d'accès à ces données, même en mode dégradé. Les données critiques sont celles mobilisées par les PCA métiers, et les données importantes sont celles qui permettront la reprise d'activité à la sortie de la crise, et le retour à un environnement normal de travail.
Assurer la sauvegarde et la sécurité des données peut entraîner des modifications dans la gestion quotidienne des données, hors période de crise. Cela va consister en des sauvegardes et archivages réguliers, éventuellement une vérification de ceux-ci. Il va par ailleurs être nécessaire de sécuriser les lieux de stockage physique des données, et éventuellement de les dupliquer. Afin d'éviter la saturation des serveurs, la croissance des volumes doit être anticipée.
Un mécanisme de restauration des données sera prévu en cas de corruption de celles-ci.
Ces différentes solutions vont conduire à la formalisation de procédures et bien souvent au recours à des prestataires de secours. Des responsables seront également désignés.
Les problématiques de sécurité et de confidentialité du SI ne doivent pas être oubliées au profit de la prévention d'un sinistre grave. Le PSI doit garantir la sécurité des accès physiques et virtuels aux SI, ainsi que leur intégrité.

En tant que partie du PCA global de l'organisation, les problématiques de surveillance et d'alerte, de gestion de crise, de communication, de sécurité des personnes, de logistique (approvisionnement en énergie notamment) et de ressources humaines sont prévus par les dispositifs de gestion de crise et de PCA global.
L'articulation entre les différentes composantes du PCA et la problématique organisationnelle sont également gérées par la gouvernance du PCA.

Le PSI devra néanmoins identifier les ressources et moyens qui lui sont nécessaires, et notamment le budget. En l'absence d'un budget dédié, il n'est pas possible de mettre en place un PSI, et celui-ci s'avère souvent conséquent. Il est défini fonction de la criticité des éléments sur lesquels porte la continuité informatique, de la taille de l'organisation, et de l'interpénétration entre l'informatique et l'activité cœur de métier. Il est important que le budget soit spécifique au PSI et non confondu avec celui de la DSI, et cela demande encore une fois un fort soutien de la Direction Générale.

Imaginer des solutions de PCA supports

Lorsque les PCA métiers ont identifié leurs besoins en services supports minimaux, les fonctions supports élaborent leur PCA en visant à assurer la fourniture de ces services minimaux en toutes circonstances, y compris en cas d'activation d'un site de repli, et même lorsque les fonctions support fonctionnent elles-mêmes en mode dégradé. Leurs objectifs de continuité doivent être cohérents avec les DMIA et PMDT définis par les métiers. Elles doivent notamment s'assurer qu'il leur est possible de fournir ces services si tous les PCA métiers sont déclenchés simultanément.
A l'instar des PCA métiers, elles doivent également prévoir la reprise d'activité en environnement normal de travail (PRA), et intégrer l'identification des acteurs avec la définition des rôles et

responsabilités, prévoir les pouvoirs et délégations de pouvoirs ainsi que le processus de prise de décision. A ces solutions, elles doivent attacher un budget.
Traditionnellement, les fonctions supports concernées par ce type de problématiques sont les Ressources Humaines, la Communication, les Moyens Généraux et Techniques (avec notamment la fourniture en énergie et fluides, fournitures et consommables), les Achats (incluant les approvisionnements et les stocks) et la Direction Administrative et Financière (dimensions juridique, comptable, trésorière, de contrôle de gestion et financière, notamment à travers les budgets). En fonction des organisations et de leur cœur de métier, les Directions Commerciale et Marketing seront considérées tantôt comme une fonction métier, tantôt comme une fonction support.

Continuité d'activité des partenaires de l'organisation

Dans le cas où l'analyse de la criticité des services en amont et en aval de l'organisation, eu égard à la continuité d'activité, ainsi que l'analyse des dispositifs de maîtrise des risques qu'ils ont mis en place pour se prémunir d'un sinistre, révèlent d'importantes défaillances, cette problématique sera traitée dans le PCA de l'organisation, à travers les PCA des métiers ou fonctions supports directement concernés par ces partenaires, appuyés par la gouvernance du PCA et de l'organisation et par l'Audit Interne.
Les solutions qui peuvent être envisagées sont une requête auprès des partenaires afin qu'ils mettent en place une démarche de continuité d'activité et en fournissent la preuve, ceci accompagné d'une clause d'auditabilité dans le contrat qui les lie à l'organisation, afin d'avoir la possibilité de s'assurer de la pertinence de leurs dispositifs.

Proposer une organisation globale du PCA

La conception des composantes du PCA que sont les PCA métiers et supports et le PSI requiert une révision globale à partir d'un contrôle de cohérence sur l'articulation de ces dispositifs entre eux, et sur l'ensemble des flux au sein de l'entreprise. Il est également nécessaire de vérifier l'intégration des procédures PCA au sein des procédures opérationnelles quotidiennes, et d'anticiper la mise en place d'une gestion de crise.
Le PCA global de l'organisation doit par ailleurs prévoir les dispositifs de sécurité et de logistique de crise qui supportent le PCA. La logistique doit notamment prévoir les sites de repli et l'organisation des transports et du déménagement vers ces sites. Une politique de communication et la documentation du PCA viennent s'y ajouter, ainsi qu'un PRA global pour le retour de l'organisation à une situation normale.
Le PCA global se charge de piloter les mesures prises pour s'assurer de la fiabilité des partenaires de l'organisation en ce qui concerne la continuité d'activité.
Il s'agira enfin de valider la conformité de toutes les composantes du PCA à la stratégie de continuité, aux objectifs et aux attentes de la Direction générale.

Cas particulier des structures complexes

Une organisation présentant une structure complexe de type multi-entité, maison-mère et filiales notamment, doit intégrer cette dimension dans la définition de sa stratégie de continuité. En effet, il est nécessaire de veiller à la conformité du PCA des filiales avec la stratégie de continuité définie par

la maison mère, et notamment à l'adéquation des moyens déployés. La maison-mère s'assurera par ailleurs que la filiale a bien mené une démarche PCA conforme à la méthodologie retenue, de laquelle cette dernière produira une documentation probante. L'objectif est de vérifier que les solutions sont pertinentes et correctement formalisées. Les bonnes pratiques préconisent en outre de tendre vers une mutualisation des moyens, et la filiale s'appuiera notamment sur les travaux du groupe pour concevoir, déployer et maintenir son PCA.
La filiale disposera néanmoins d'une capacité décisionnelle et budgétaire propre, lui permettant de gérer de manière autonome toute crise.

Dimension préventive du PCA

La mise en œuvre d'un PCA dans une organisation peut être l'occasion, parallèlement à l'objectif de réduction de l'impact des sinistres, de lancer ou de renforcer des mesures de prévention pour diminuer la probabilité de survenance d'un sinistre.
Cela va notamment se traduire par l'intégration des problématiques de continuité dans les nouveaux projets dès leur lancement. Ce sont bien souvent des mesures de bon sens.
L'éventuelle perte de connaissances et savoirs-faire de l'organisation peut également être anticipée, en prévoyant notamment un moyen de les recouvrir s'ils sont perdus.
Cependant, et malgré toutes ces précautions, un risque résiduel de survenance d'un sinistre demeure non couvert, et une démarche PCA reste nécessaire.

c) Phase 3 : Validation de l'étape

La qualité de cette étape de définition des activités critiques et de stratégie de continuité conditionne la réussite d'un projet PCA. Sa validation est donc essentielle.
La formalisation de la cartographie des processus et de la cartographie des risques sont soumis pour avis au Management des Risques et au Contrôle Interne (et non à l'Audit Interne, pour conserver l'objectivité et l'indépendance nécessaires aux audits ultérieurs) et à la validation des comités opérationnel et de pilotage du PCA.
Les analyses d'impact d'une interruption pour chaque activité sont validées par le comité opérationnel du PCA, qui valide également les analyses de criticité des services en amont et aval de l'organisation et les analyses des dispositifs de maîtrise des risques déjà existants pour les activités et les partenaires de l'entreprise.
Le comité de pilotage du PCA valide quant à lui les besoins en continuité des métiers et du SI, les solutions de secours prévues par les PCA métiers et le PSI ainsi que l'identification des moyens et ressources qui leur sont nécessaires, à travers les PCA des fonctions supports et les budgets de l'ensemble des plans. Il révisera également l'organisation globale du PCA et les mesures prévues pour s'assurer de la continuité d'activité assurée par les partenaires de l'entreprise, et les éléments ayant trait à la sécurité et à la logistique de crise (site de repli notamment).
A ce stade, les solutions de secours ne sont que des propositions, et les ressources nécessaires pour les mettre en œuvre sont estimées par les opérationnels et fonctions supports, et indicatives. Il peut par ailleurs y avoir plusieurs propositions de solutions pour un même objectif de continuité. Elles feront l'objet d'une étude plus approfondie, et d'une décision finale.
Sans cette validation préalable des propositions, le projet PCA peut être mis en attente.

1.3.1.3 Etudier et choisir les solutions envisageables

a) Phase 1 : Etude de faisabilité et chiffrage des solutions envisageables

Lorsque la stratégie de continuité et les propositions de solutions de secours sont formalisées et validées, celles-ci sont à étudier dans le détail. Les solutions font tout d'abord l'objet d'une étude de faisabilité et d'un chiffrage.
L'étude de faisabilité et le chiffrage des solutions doivent être envisagées selon les critères techniques et financiers.

Critères techniques

L'étude de la faisabilité technique vise à répondre aux questions suivantes :

- Est-ce que l'organisation a les moyens de le faire ? (ou possibilité de les acquérir)
- Est-ce que l'organisation sait le faire ? (ou possibilité d'apprendre)
- Est-ce qu'il est autorisé de le faire ?

La faisabilité globale de la solution s'évalue en analysant la suffisance et la disponibilité des ressources humaines, à la fois en termes de nombre d'employés et de compétences spécifiques, et notamment en ce qui concerne la coordination avec les PCA des autres activités critiques. Il s'agira en effet de s'assurer que les ressources de l'organisation permettent de mettre en œuvre les solutions de toutes les activités critiques simultanément.
Il est également nécessaire d'évaluer la capacité de l'organisation à mettre en œuvre la solution envisagée, en cherchant notamment si elle dispose des savoirs-faire nécessaires, si les techniques et technologies sont disponibles, si elle détient les matériels et outillages, si ses capacités de stockage sont suffisantes, quelle est la fiabilité des prestataires, fournisseurs et partenaires, quelle est la qualité des services supports sur lesquels s'appuie cette activité. Enfin, l'étude va porter sur la conformité de la solution à la réglementation en vigueur et aux directives des instances de tutelle, régulateurs, ou toute instance de surveillance.

L'étude de faisabilité technique doit par ailleurs porter sur l'éventuel site de repli, avec une analyse des infrastructures techniques existantes, ainsi que sur coordination prévue avec les prestataires de secours, et la fiabilité de ceux-ci.

Critères organisationnels

L'étude de faisabilité organisationnelle vise à répondre à la question :

- Est-ce que l'organisation appropriée a été prévue pour pouvoir le faire ?

Il s'agit ensuite d'évaluer la faisabilité du volet organisationnel des solutions proposées. L'étude va porter sur les procédures et modes opératoires formalisés, le processus de prise de décision proposé, les acteurs et la répartition des rôles, les responsabilités et pouvoirs envisagés, l'articulation prévue avec les SI et les services supports, en particulier celle prévue avec les Moyens Généraux et Techniques, et enfin la logistique et la sécurité prévues.

Critères financiers

L'étude de faisabilité financière vise avant tout à chiffrer les solutions envisagées, à la fois pour les PCA métiers et fonctions supports, et pour le PCA global de l'organisation.
Ce chiffrage permettra de répondre aux questions :

- Le coût de la solution est-il bien inférieur au coût de l'interruption ?
- L'organisation dispose- t-elle des ressources financières suffisantes pour pouvoir le faire ?

Les solutions envisagées seront estimées à la fois en termes d'investissement sur le projet (conception et déploiement) du PCA, mais aussi de financement de la maintenance (MCO : Maintien en Condition Opérationnelle) du PCA chaque année. Par conséquent, le chiffrage doit prendre en compte des coûts futurs en constante évolution, et en cherchant à en déterminer les coûts cachés. L'estimation financière doit être étendue au choix des prestataires de secours, en particulier en ce qui concerne les SI et les sites de repli. Le coût des solutions doit ensuite être rapproché du coût d'une interruption. Il sera par ailleurs nécessaire de déterminer là ou les directions auxquelles sera rattaché le budget PCA.

b) Phase 2 : Evaluer la pertinence des solutions envisagées

L'évaluation de la pertinence des solutions envisagées vise à répondre à la question :

- L'organisation a-t-elle raison de vouloir le faire ?

La pertinence des solutions envisagées se mesure à travers le degré de réponse aux objectifs de continuité. Ainsi, il s'agira de s'assurer que les solutions permettent de maîtriser les risques et de garantir la continuité puis la reprise des activités en cas de survenance d'un sinistre, c'est-à-dire la gestion de crise puis la sortie de crise et le retour à un environnement normal de travail.
Il sera par ailleurs nécessaire de vérifier que le coût de mise en place et de déploiement des solutions n'est pas supérieur à l'impact, notamment financier, d'une interruption des activités.
Enfin, il s'agira de mesurer dans quelles dimensions ces solutions répondent aux attentes de la Direction Générale et aux obligations règlementaires.

c) Phase 3 : Prise de décision : Choix des solutions

Les différentes études menées permettent d'évaluer l'opportunité et la faisabilité de la mise en place des différentes solutions de continuité. La décision finale de les mettre en place revient aux organes de pilotage du PCA, le comité opérationnel et le comité de pilotage, sur la base du résultat des études.
Le PCA ainsi retenu sera ensuite soumis au CHSCT (Comité d'Hygiène, de Sécurité et des Conditions de Travail) ainsi qu'aux instances représentatives du personnel.
Enfin, le PCA est porté à la connaissance de la Direction Générale, qui validera les moyens déployés pour sa réalisation à hauteur des objectifs fixés.

1.3.1.4 Mettre en place une base documentaire

a) Base documentaire

La formalisation, la documentation et la conservation de tous les éléments qui composent le PCA est essentielle, ce qui fait de la base documentaire un pilier indispensable et incontournable à tout PCA. La base documentaire doit être adaptée au contexte, être à jour, testée et disponible en cas de sinistre. Elle regroupe tous les livrables liés au PCA.

b) Les livrables PCA incontournables

Livrables organisationnels :

- Charte du PCA
- Fiches de poste et désignation des acteurs PCA
- Composition, pouvoirs et périodicité des organes de pilotage du PCA
- Ordres du jour et comptes-rendus des réunions des organes de pilotage du PCA
- Lettre d'engagement de la Direction Générale
- Cartographie des processus
- Cartographie des risques
- Politique de communication

Livrables liés à la conception du PCA :

- PCA global de l'organisation
  - Stratégie de continuité globale
    - ➔ Objectifs et attentes de la Direction Générale
    - ➔ Procédures de sécurité et de logistique de crise
    - ➔ Procédures de retour à la normale
    - ➔ Articulation globale des composantes du PCA
    - ➔ Mode d'archivage de la documentation du PCA
  - Validation de la stratégie de continuité globale (Comité de pilotage du PCA, Direction Générale)
  - Analyse de la criticité des services en amont et en aval de l'organisation et procédures liées
- PCA métiers et fonctions supports
  - Expression des besoins en continuité
    - ➔ Analyses d'activité
    - ➔ Analyses des impacts des interruptions (DMIA / PMDT)
    - ➔ Analyse des dispositifs de maîtrise des risques existants
    - ➔ Stratégie et objectifs de continuité (RTO / RPO)
    - ➔ Procédures de secours métiers
    - ➔ Procédures de reprise d'activité métiers
    - ➔ Moyens nécessaires (dont prestataires externes)
    - ➔ Procédures de secours supports
    - ➔ Procédures se reprise d'activité supports
    - ➔ Identification du personnel concerné et des parties prenantes

- Environnement technique
  - PSI (Plan de Sauvegarde Informatique)
    - ➔ Contrats de service métiers
    - ➔ Analyse des risques et des impacts
    - ➔ Analyse des dispositifs de maîtrise des risques existants
    - ➔ Stratégie et objectifs de continuité informatique
    - ➔ Procédures de secours
    - ➔ Procédures de sauvegarde des données
    - ➔ Procédures de reprise informatique
    - ➔ Identification du personnel et des parties prenantes concernées par le PSI
    - ➔ Moyens nécessaires (dont prestataires externes)

    (Outil de Gestion Electronique des Documents du PSI)
  - Site de repli et matériel de secours
    - ➔ Dossier de mise en place et de gestion
    - ➔ Procédures d'activation (déménagement)
- Validation de toutes les stratégies et objectifs de continuité
- Validation des procédures de secours et de retour à la normale retenues
- Validation des moyens déployés

Livrables liés au déploiement du PCA :

- Procédures de gestion de crise
  - Surveillance, alerte et escalade
  - Déclenchement et pilotage du PCA
  - Gestion de crise
  - Comptes-rendus de réunions de cellule de crise
  - Journaux de bord de gestion de crise
  - Protocoles de communication de crise
- Test technique du PCA
  - Modes opératoires
  - Retour d'expérience et journal de bord
  - Axes d'améliorations et recommandations

Livrables liés à la maintenance du PCA :

- Documents d'organisation des tests du PCA
- Plan de tests pour l'année et ressources allouées
- Plan de test pluriannuel
- Rapports et journaux de bord des tests
- Axes d'amélioration, recommandations et leur suivi (plans d'action)
- Rapports des audits du PCA
- Recommandations d'audit, plans d'actions et leur suivi
- Traçabilité des mises à jour des évaluations financières
- Traçabilité des mises à jour des procédures

Livrables liés au reporting PCA :

- Suivi des indicateurs

- Tableaux de bord
- Plans d'actions
- Référentiels
- Bilans des tests et audits
- Rapports annuels d'activité
- Synthèses des mises à jour

1.3.1.5 Prévoir une politique de communication

La dimension de communication est l'un des facteurs clés de réussite du PCA. Elle est nécessaire à la fois en amont afin que les acteurs et parties prenantes concernées par le PCA connaissent le dispositif, mais également dans le cadre d'une crise, principalement pour rassurer les inquiétudes du public, et sauvegarder l'image de l'organisation. Il est essentiel pour une organisation de maîtriser sa communication en toutes circonstances.
Les situations de crise sont souvent caractérisées par des prises de parole en tous sens. L'organisation doit définir une politique de communication et désigner un porte-parole, afin de délivrer un message unique et cohérent en interne comme en externe.
Les porte-paroles doivent être entraînés et formés, et le message diffusé approuvé par le RPCA et la gouvernance du PCA et de l'organisation, ou à minima par la cellule de crise.
La désignation du porte-parole, les messages communiqués et l'éventuelle préparation des messages à l'avance montrent que l'organisation est prête à réagir à une crise.

a) <u>Communication Interne</u>

Au-delà de la nécessaire information et formation des acteurs clés chargés du déploiement du PCA, qui sera abordée plus en détail dans le volet de mise en œuvre du PCA, la communication interne doit s'adresser à l'ensemble des collaborateurs de l'organisation, dans une perspective de sensibilisation du personnel et d'intégration du dispositif dans la culture de l'organisation.

En amont de la survenance potentielle d'une crise, cette communication sert deux objectifs essentiels. Tout d'abord, la sensibilisation des collaborateurs aux problématiques de continuité rend les dispositifs mieux maîtrisés et plus efficaces, mais permet également de rassurer les salariés quant à la capacité de l'organisation à faire face à une crise. Bien informés, chacun saura trouver sa place et son rôle rapidement et facilement en cas de sinistre. Cela nécessite donc d'informer également les salariés hors activités critiques qui ne sont pas directement concernés par le déploiement du PCA.
Le PCA doit faire l'objet d'une communication régulière et sur le long terme dès le début de sa conception. Le personnel doit comprendre que le PCA est la volonté de la Direction Générale et qu'il concerne toute l'entreprise, aujourd'hui et pour longtemps. L'information permet d'éviter une mauvaise compréhension du PCA et de répondre à certaines questions que se pose le personnel. Il s'agit notamment de présenter le PCA, ses enjeux et ses objectifs, le périmètre qu'il couvre et les solutions de continuité et de reprise d'activité, mais aussi de définir ce qu'est une activité critique, justifier la sélection des activités critiques qui a été faite, et expliquer les conséquences d'un sinistre pour le personnel hors activités critiques. L'organisation et la logistique autour du déploiement du PCA (horaires, site de repli, transports, restauration…) doit également être explicitée.

Il convient de prévoir un accès à l'information et des supports de communication adaptés, que le personnel soit impliqué ou non dans le déploiement du PCA. Quelques bonnes pratiques consistent en une lettre de la Direction Générale à l'ensemble du personnel lors du lancement du projet, ainsi qu'une présentation du projet PCA et des points d'avancement devant les instances représentatives du personnel et le CHSCT.
Il pourrait également être imaginé un site intranet dédié au PCA, qui pourrait ensuite évoluer et devenir un lieu de stockage des procédures et autres documents qui formalisent le PCA, ainsi qu'un lieu d'échange où le personnel pourrait poser des questions et une plateforme permettant d'organiser les tests du PCA.
Par ailleurs, la Direction Générale peut communiquer sur les grandes étapes d'avancement du projet PCA, pour annoncer la formation du personnel impliqué et les tests du PCA, et pour remercier le personnel après les tests en en donnant les résultats.
En outre, la communication interne, pilotée par le RPCA et les organes de gouvernance du PCA et de l'organisation, peut être relayée auprès des salariés par le biais des CCA (Correspondants de Continuité d'Activité).
Certaines organisations vont choisir une diffusion orale transitant par les différents niveaux de management, qui présente l'intérêt d'être plus interactive et plus personnelle, lorsque d'autres vont préférer une diffusion uniforme de messages généraux, afin que chacun dispose du même niveau d'information et de compréhension, sans déperdition d'informations au fur et à mesure de la retransmission. Ces messages peuvent éventuellement être traduits pour une population non initiée.

Lors de la survenance d'une crise, la communication interne répond à d'autres enjeux. Elle doit tout d'abord appuyer et rendre possible le déploiement du PCA, à travers l'information des employés sur la situation et la distribution de consignes.
Par ailleurs, focalisées sur les métiers et le déploiement des solutions, les organisations en oublient la notion de perception de la crise. L'aspect humain et psychologique est primordial dans le cadre d'un PCA, et une organisation ne remplit pas son rôle si elle ne rassure pas les inquiétudes de ses salariés. Cette communication est alors pilotée et mise en œuvre par la cellule de crise.

b) Communication Externe

La communication externe autour du PCA est tout aussi importante que la communication interne, tant en situation de crise qu'en amont de la survenance de celle-ci. Elle sert essentiellement des objectifs d'image de l'organisation, recherchant sa promotion et son maintien.

En dehors des situations de crise, la communication externe vise essentiellement à promouvoir l'organisation. En effet, auprès des partenaires, des clients et du grand, elle sert à présenter la capacité de l'organisation à faire face à l'éventualité d'un sinistre, en fournissant la garantie de la continuité d'un service minimum en toutes circonstances. Cela peut notamment constituer un avantage concurrentiel intéressant. Elle s'adresse également aux organismes de contrôle et aux instances de tutelle, afin de montrer que les exigences et les bonnes pratiques en la matière sont appliquées et respectées. Cette communication externe peut être obligatoire, ou résulter d'une volonté de prévention, par exemple à l'attention des populations vivant à proximité d'un site sensible. La stratégie de ce type de communication est élaborée par les organes de gouvernance du PCA et de l'organisation, et mise en œuvre par les équipes de communication externe ou de

marketing. Elle peut apparaître dans les campagnes de communication ou publicitaires, dans les newsletters envoyées aux partenaires, valorisée sur le site internet de l'organisation…

Lors d'une crise, le pilotage de la communication externe est transféré à la cellule de crise, qui se chargera de l'application du protocole de communication externe préalablement établi, de la validation des messages avant leur diffusion et de la coordination des porte-paroles et des médias. Il existe une vraie problématique liée aux médias, car les messages qu'ils transmettent échappent au contrôle de l'organisation. L'organisation conserve cependant la maîtrise de ses propres propos, et c'est sur ces éléments qu'elle doit concentrer ses efforts. L'objectif est la préservation de l'image de l'organisation, en cherchant à rassurer le public sur la situation, l'informer sur l'évolution des évènements jusqu'à la résolution de la crise et le retour à une situation normale. A l'issue de la crise, une campagne de communication peut présenter le retour d'expérience et les actions entreprises pour se prémunir contre la reproduction de cette situation à l'avenir.

Une bonne maîtrise de la communication externe est un point essentiel de contrôle, et il est nécessaire d'y associer les moyens adéquats. En effet, cette maîtrise permet d'éviter de monter des systèmes coûteux, car lorsqu'un incident ne nuit pas l'image de l'organisation, certains risques deviennent plus tolérables et donc les dispositifs pour les maîtriser superflus.

c) Problématiques de confidentialité

Le PCA revêt un certain caractère stratégique, puisque traitant des risques auxquels une organisation est vulnérable, et s'inscrivant dans ses objectifs stratégiques. Une diffusion publique de ces éléments, en particulier à ses concurrents, peut s'avérer néfaste pour l'organisation. En ceci, certains aspects du PCA vont être confidentiels. Il convient de classifier les informations selon trois niveaux de confidentialité. Le premier niveau regroupera les informations non classifiées, qui peuvent faire l'objet d'une communication externe à l'entreprise. Un second niveau se limitera à une diffusion restreinte, interne à l'organisation, dont la diffusion en externe pourrait lui porter préjudice. Le troisième niveau concerne les informations réellement confidentielles, dont la diffusion se limite à leurs seuls destinataires.
Des dispositifs de protection des informations doivent par conséquent être mis en place, en particulier à travers la sécurisation du système d'information. Une forte sensibilisation du personnel concerné est également essentielle.
Cette classification des informations permet de préserver les intérêts de l'organisation, mais peut néanmoins nuire à l'appropriation du PCA par une partie du personnel.

1.3.2 La mise en œuvre du PCA : Le déploiement

1.3.2.1 Mise en place d'une gestion de crise

La gestion de crise constitue l'une des composantes essentielles d'un plan de continuité d'activité, qu'il est tout aussi essentiel de maîtriser et donc de prévoir. En effet, si la conception et la documentation d'un plan de continuité d'activité permet à une organisation de prévoir la réaction qu'elle aura en cas de crise, c'est la gestion de crise qui permettra non seulement d'anticiper et de détecter la survenance de cette crise pour enclencher la réaction prévue, mais également la supervision pendant la crise, sans compter l'organisation de la sortie de crise vers un retour à la normale.
La gestion de crise nécessite une bonne appréhension de la situation, des évènements et de l'environnement auxquels est soumise l'organisation, afin d'orchestrer la réaction adéquate. La gestion du temps en est un facteur clé de succès.
Ainsi, elle se compose de plusieurs volets, le premier consistant à effectuer une veille permanente, en particulier sur la remontée des incidents, afin de détecter au plus tôt une éventuelle anomalie présageant la survenance d'un sinistre de grande envergure. Avec cette détection doit être prévu un dispositif d'alerte et d'escalade, conduisant progressivement à la déclaration d'état de sinistre et le déclenchement du plan de continuité d'activité. Par la suite, la gestion de crise elle-même supervisera le déploiement du PCA, à travers notamment la gestion des imprévus n'ayant pas été envisagés lors de sa conception. C'est également à travers la gestion de crise que sera mise en œuvre la communication interne et externe autour de la continuité d'activité. Le dernier volet vise à garantir la sortie de crise et le retour à un environnement normal de travail, avec notamment la surveillance de l'évolution de la situation tout au long de la crise, et l'identification du moment où l'organisation est prête à enclencher son plan de reprise d'activité.
A l'instar des autres composantes du PCA, la gestion de crise d'appuie sur des procédures documentées.

a) <u>Formation d'une cellule de crise</u>

Dans un premier temps, la nomination de la personne chargée de piloter la cellule de crise est très importante. Celle-ci est désignée par le RPCA, approuvée par le Comité de Pilotage du PCA.
Dans le cadre d'une organisation de taille importante, il pourra être envisagé la mise en place d'une cellule de crise décisionnelle, chargée d'assurer le pilotage et la coordination de cellules de crises opérationnelles déployées dans l'organisation, en fonction des différents sites ou activités notamment. Il est cependant primordial de veiller à ce qu'une réelle interface et coordination existent entre ces différentes cellules, avec une communication rapide et efficace. Cette transversalité n'est pas toujours naturelle, car chacun reste spécialiste de son domaine et ne connait pas les champs de compétences des autres. Les différents acteurs de la gestion de crise doivent se connaître et connaître leurs enjeux respectifs : les enjeux techniques, de continuité, d'une part, et les enjeux commerciaux et d'image, d'autre part.
Les dispositifs de gestion de crise peuvent s'avérer coûteux, et leur criticité peut requérir le recours à une expertise externe.

b) Dispositif de veille, de remontée et de gestion des incidents

Le rôle de ce dispositif, sous la responsabilité de la cellule de crise et bien souvent négligé, est néanmoins primordial. En effet, c'est l'anticipation et la détection de la crise qui permettent le succès de la continuité d'activité, avec une bonne réactivité et une bonne gestion du temps.
La veille est matérialisée par le suivi et la surveillance d'un certain nombre d'indicateurs, préalablement définis comme permettant de repérer les dysfonctionnements. Généralement, l'un de ces indicateurs sera la remontée et la gestion des incidents, leur fréquence et leur gravité. Le dispositif de veille, de remontée et de gestion des incidents comprend par ailleurs les procédures d'astreinte et de permanence. Il faut cependant différencier les astreintes techniques des astreintes de veille visant à permettre une meilleure réactivité face à la crise. Cette veille peut également porter sur des données règlementaires, concurrentielles, médiatiques…
Lors de remontées d'incidents, émanant des activités opérationnelles comme support, ainsi que lors de l'évolution des indicateurs précurseurs à une éventuelle crise, l'évaluation de la gravité de ces éléments doit avoir été prévue, afin que soit possible leur analyse par la cellule de crise. La mesure de la gravité d'un incident peut se baser sur les niveaux de services minimums définis lors de la conception du PCA : Si l'incident menace la capacité de l'organisation à assurer ce niveau de service minimum, la gravité a atteint un certain niveau. La cellule de crise adapte sa réaction au niveau de gravité ainsi déterminé.
La gestion des incidents va chercher à traiter les évènements indésirables de faible envergure, ne nécessitant pas le déclenchement du dispositif d'alerte, afin qu'ils ne dégénèrent pas jusqu'à provoquer une crise.
Lorsque le dispositif de veille détecte un évènement catastrophique ou à fort potentiel de crise, la cellule de crise déclenche le dispositif d'alerte et d'escalade.
Une documentation de cette veille est nécessaire, en particulier la création d'une base d'incidents conservant un historique.

c) Dispositif d'alerte et d'escalade

La réactivité d'une organisation est l'un des facteurs clés de succès de la continuité d'activité d'une organisation. Une fois le dispositif d'alerte enclenché, il est essentiel pour une organisation d'avoir préalablement établi les protocoles d'alerte et d'escalade.
Dans certains secteurs d'activité, le dispositif d'alerte est règlementé et exige l'alerte des autorités ou des instances de tutelles des évènements détectés. Cela relève du rôle de la cellule de crise dans le cadre de son dispositif d'alerte. En interne, l'alerte est communiquée à la Direction Générale et au personnel, et le suivi des indicateurs est renforcé. En fonction des seuils successifs atteints par les indicateurs vers une situation de crise, la cellule de crise communique sur l'escalade, jusqu'à déclarer la situation de crise et déclencher le plan de continuité d'activité.
Son rôle évolue alors vers une gestion de la crise.

d) Gestion de la crise et de la communication

Gestion de la crise

Par définition, chaque crise est unique. La qualité de la gestion qui en sera faite repose en partie sur la capacité d'adaptation dont saura faire preuve l'organisation, notamment face aux imprévus qui n'avaient pas été imaginés lors de la définition de la stratégie de continuité. La gestion de crise vise à être capable de faire face à tous types d'évènements.
Son rôle va être primordial au moment de la transition vers le mode dégradé et les procédures de continuité, afin de s'assurer que la crise ne créée pas de panique et que chacun assure son rôle, que les dispositifs soient déployés tels qu'ils ont été prévus.
La cellule de crise devra donc notamment organiser le processus de prise de décisions et le pilotage des situations dans toutes leurs composantes (opérationnelles, juridiques, commerciales, RH et communication).
Elle veillera à développer un langage commun avec les acteurs du PCA, car ils ont vocation à travailler en étroite collaboration. La cellule de crise va donc suivre le déploiement du PCA, et surveiller l'évolution de la situation à travers ses indicateurs de veille. Elle intervient pour la gestion des imprévus, et doit donc être en mesure de les détecter grâce à une vigilance constante.

La communication de crise

Chargée de piloter la communication de crise en interne et en externe, la cellule de crise se charge de tenir un journal de bord, qui servira de base au retour d'expérience sur la crise. La quantité d'informations produites et échangées au cours d'une crise requiert un suivi et une documentation très réguliers. Par ailleurs, la capitalisation d'informations vécue en crise peut permettre de contrer d'éventuels contentieux susceptibles de survenir plusieurs années après la crise vécue.
En interne, elle doit informer et distribuer les consignes au personnel lors de l'enclenchement du PCA, assurer le reporting auprès de la Direction Générale et du Comité de Pilotage PCA sur la situation de la crise, et lui fournir l'ensemble des informations qu'ils exigent. Elle doit également orchestrer la communication descendante vers le personnel, à la fois les acteurs impliqués dans le déploiement du PCA et ceux qui ne sont pas directement concernés. Son rôle va consister à élaborer ou à minima valider les messages qui seront transmis par le porte-parole et via les différents moyens de communication retenus.
En externe, la cellule de crise va, de la même manière, valider voire élaborer les messages portés par l'entreprise, éventuellement gérer les relations avec les médias et les réseaux sociaux, afin de s'assurer que le message transmis est unique, cohérent et pertinent, préservant ainsi l'image de l'entreprise.

e) Sortie de crise et retour à une situation normale

A travers sa surveillance de l'évolution de la crise, la cellule de crise sera à même d'identifier l'amorçage de la sortie de crise, et ainsi déclencher le plan de reprise d'activité, qu'elle accompagnera et suivra de la même manière que le plan de continuité d'activité.
La sortie de crise sera ensuite officiellement déclarée, accompagnée de l'information en interne et en externe des acteurs et parties prenantes, le remerciement de tous ceux qui ont participé à la

continuité et la reprise d'activité, ainsi que le retour de la fonction de Direction aux mains de la Direction Générale.
Lors du retour à une situation normale, les causes du sinistre devront être explicitées et traitées, afin de réaliser un retour d'expérience enrichissant. Ce retour d'expérience devra également porter sur la réaction de l'organisation au sinistre, et en tirer des pistes d'amélioration du PCA, de la même manière que cette réflexion est menée à la suite des tests du PCA.
Il est essentiel de tirer les enseignements d'incidents, de dysfonctionnements ou de crises, afin d'éviter leur répétition. La culture du débriefing est un bon moyen d'évaluer les dispositifs de manière pertinente.

1.3.2.2 Mise en place des sites de repli et du matériel de secours : Logistique de crise

Un site de repli est un site alternatif au site principal, tenu prêt pour utilisation lors de la survenance d'un évènement menaçant la continuité d'activité. Il sera activé en cas de sinistre grave privant l'organisation de son site principal, et devra permettre de soutenir le niveau d'activité minimum défini dans la stratégie de continuité, correspondant au niveau de service minimum dont il faut maintenir la continuité en toutes circonstances. Il doit par conséquent prévoir dans sa conception les espaces de travail, l'acquisition du matériel et des technologies nécessaires, en particulier les infrastructures de télécommunication, de réseaux et systèmes informatiques, ainsi que d'alimentation en énergie et fluides. Ces équipements doivent être opérationnels pour une activation soudaine à tout moment, en veillant à ce que les coûts de maintien en attente ne soient pas excessifs. Il sera par ailleurs nécessaire d'y constituer un stock minimum de fournitures de première nécessité.

Avec la mise en place d'un site de repli doit être prévue la logistique de déménagement des activités du site principal vers ce site, et de moyens de transports des collaborateurs vers le site. Sachant que l'activation du site se fera dans l'urgence et dans un contexte de crise, il est essentiel que les procédures soient prévues, et qu'elles garantissent la sécurité du personnel.
Par ailleurs, des infrastructures supplémentaires pourront être envisagées afin d'accompagner et de favoriser la présence du personnel sur le site de repli en période de crise, telles qu'un restaurant, un éventuel hébergement, des services de gardes d'enfants… Le déploiement d'une cellule psychologique et d'un centre de soins peuvent être à prévoir, en fonction du sinistre subi par l'organisation.

Un site de repli peut être un bâtiment indépendant construit affecté dans un seul objectif de continuité d'activité, comme il peut être un site utilisé au quotidien pour des opérations normales, mais capable de s'adapter rapidement pour pouvoir accueillir une autre activité critique de l'organisation dont le site principal serait sinistré.

1.3.2.3 Protection du personnel et sécurité

Le déploiement du Plan de Continuité d'Activité ne doit pas négliger la responsabilité de l'organisation de protection de son personnel. Des plans de protection du personnel doivent être mis en place, pouvant prévoir l'évacuation des personnes, un centre de secours et de soins, un support

psychologique, le transport vers le site de repli, l'alimentation et éventuellement l'hébergement, ou encore un système de support aux familles comme l'organisation de garde d'enfants.

1.3.2.4 Implication des partenaires indispensables

Dans le cas où les PCA métiers ou le PSI prévoient dans leurs solutions le recours à des prestataires externes, ces partenariats doivent être formalisés dans des contrats spécifiques, qui prévoient notamment le mode d'activation des solutions de secours en collaboration et le lien entre le prestataire et la cellule de crise de l'organisation. Les interlocuteurs au sein du prestataire comme de l'organisation doivent être identifiés préalablement à la survenance d'un évènement.

1.3.2.5 Informer et former les acteurs impliqués

Le succès du déploiement du PCA repose en grande partie sur l'appropriation que se seront faite les responsables des métiers et des équipes techniques du dispositif. Idéalement, cette appropriation s'étend aux sous-traitants et fournisseurs (en particulier les prestataires de secours), afin que chacun maîtrise bien les procédures à enclencher en cas de survenance d'une crise et le rôle qu'il doit assurer dans ce cadre. Cela garantit à la fois la réactivité de l'organisation et la qualité de sa réaction.
L'appropriation du PCA par les acteurs (internes et externes) passe par leur sensibilisation, leur information, leur formation, et les exercices d'entrainements qui seront réalisés. La sensibilisation et l'information est réalisée via la communication interne et externe en amont de la survenance d'une crise, mais la formation et les exercices sont à prévoir séparément.

a) <u>Identification des acteurs à former</u>

Dans un premier temps, il convient d'identifier les acteurs concernés par le déploiement du PCA. En interne, il s'agira du personnel identifié dans les procédures métiers ou fonction et dans les fiches de poste. Cela doit inclure le personnel impliqué sur les sites de repli. Avec les partenaires, des réunions avec les interlocuteurs identifiés permettent de définir les axes et la stratégie des formations qu'ils dispenseront ensuite à leur personnel.

b) <u>Organisation de la formation</u>

La formation est effectuée de préférence par le RPCA ou toute personne ayant une connaissance suffisante du dispositif et du détail des procédures pour répondre aux questions des participants. La présence d'un sponsor (DRH, directeur métier, membre de la Direction Générale) peut être intéressante pour initier les 5 premières minutes de la formation, afin d'en appuyer la légitimité et l'importance.
Il est recommandé de réaliser la formation par métier ou par fonction avec un nombre restreint de participants par session, pour favoriser les échanges. La formation est en effet souvent la seule opportunité de répondre aux questions du personnel et de recueillir leurs réactions avant le premier test du PCA avec une mise en situation.
La formation est réalisée une première fois lors de la mise en place du projet PCA par l'organisation, puis est mise à jour chaque année parallèlement à la mise à jour du dispositif, à la fois pour intégrer les modifications à la formations et pour former le nouveau personnel impliqué dans le PCA.

c) Contenu de la formation

La formation doit impérativement couvrir certains points, à minima :

- L'explication de la stratégie de continuité des activités :
  - Le choix des activités critiques
  - Les impacts d'une interruption du service ou de la fonction concernée sur l'entreprise
  - Le délai maximum d'interruption acceptable et la perte maximale de données tolérable
  - Le niveau de service ou de production minimum que le service ou le métier doit assurer
  - Les ressources et moyens prévues pour le déploiement des solutions
- La présentation du site de repli :
  - Localisation, plan d'accès, photos du site de repli, plan d'installation des services sur le site
  - Organisation du repli (sécurité, horaires, règlement, infrastructures)
  - Transport et logistique prévus
- La rémunération associée au PCA :
  - Remboursement de frais
  - Primes éventuelles
- Les procédures détaillées du service ou du métier :
  - Modes opératoires, rôles et responsabilités des acteurs
  - Processus de prise de décision
  - Obligations de documentation et de reporting
- La vie du dossier PCA :
  - Tests annuels (planning, organisation)
  - Mises à jour des procédures et intégration du nouveau personnel

d) Exercices

Afin de compléter la formation, il est nécessaire d'organiser des exercices pratiques, avec une simulation de déploiement du dispositif. Seules les personnes ayant participé à la formation peuvent ensuite participer à ces exercices.

1.3.2.6 Implication et support de la Direction Générale

Impliquée dès le commencement du projet PCA, avec notamment la validation de la stratégie de continuité et des moyens alloués, la Direction Générale a également un rôle à jouer lors du déploiement du PCA.
Le déploiement du Plan de Continuité d'Activité doit être porté par la Direction Générale pour que celui-ci soit optimal. Il s'agit en effet d'une démarche transverse et commune à toute l'organisation, qui doit s'inscrire dans sa culture et mobiliser tout le personnel. Chacun doit être sensibilisé à l'importance de la démarche et y adhérer, afin que la réaction de l'organisation à la survenance d'un sinistre soit optimale. Le positionnement de la Direction Générale doit intervenir dès le

déclenchement du PCA, afin de rassurer et guider les employés. C'est cette intervention qui va présenter et légitimer le pilotage effectué par la cellule de crise.
La Direction Générale donne le ton et fait preuve d'une exemplarité qui rassurera et motivera le personnel. Elle garantit une unicité et une cohérence de l'information, de la communication et du pilotage pendant la crise en déléguant temporairement les fonctions de Direction à la cellule de crise. Elle montrera son implication en étant destinataire des reportings PCA, en remerciant et valorisant le personnel mobilisé par le dispositif, et en présentant les retours d'expérience.

1.3.2.7 Mise en place de "mallettes de crise"

Les mallettes de crise sont des boites à outils à destination des responsables de processus critiques qui sont chargés de déployer des PCA métiers en cas de survenance d'un sinistre. Les utilisateurs des mallettes de crise sont répertoriés et font l'objet d'un contrôle d'utilisation. Ils sont en mesure d'en justifier l'accessibilité permanente.
Elles contiennent les éléments indispensables au maintien de la continuité d'activité en cas d'incident et à la bonne reprise de l'activité. Elles peuvent être différentes, revêtir des formes variées et s'adapter à leurs utilisateurs, mais le tronc commun de leur contenu est défini par les organes de gouvernance du PCA. Les bonnes pratiques entendent qu'elles contiennent les procédures et modes opératoires relatifs au PCA du métier à déployer, l'identification et les coordonnées du personnel à mobiliser et des interlocuteurs à contacter (RPCA, cellule de crise…), les clés et les moyens d'accéder au site de repli, et éventuellement un téléphone et un poste informatique d'astreinte et du matériel de première nécessité (trousse de secours, lampes de poche…).
Le contenu des mallettes de crise doit être revu annuellement et éventuellement mis à jour en conséquences de la mise à jour du PCA et de ses procédures.

1.3.2.8 Premier test du PCA et validation

L'exercice est la seule preuve permettant de s'assurer que l'ensemble de la démarche a été effectué correctement. Sans exercice, il est possible de prévoir, voire de financer des solutions, mais sans savoir si celles-ci fonctionnent. L'exercice présente toutefois des risques et il se décide souvent au plus haut niveau.

a) <u>Organisation et conception du test</u>

Le premier test technique du PCA est réalisé dans le cadre de son déploiement, et doit porter sur l'ensemble des composantes du PCA, à savoir le PCA et le PRA globaux de l'organisation, chaque PCA et PRA des métiers et fonctions support, le PSI et la gestion de crise, en impliquant les éventuels partenaires, fournisseurs et prestataires. Il vise à en finaliser la préparation, en décelant les dysfonctionnements qui n'auraient pas été envisagés lors de la conception des dispositifs, et à valider son efficacité. Ce test s'appuie sur un cahier des charges qui prend en compte les attentes de tous les acteurs concernés.

Plusieurs types de tests sont réalisés successivement. Tout d'abord, on réalisera un exercice sur table, où les procédures sont examinées avec les intervenants afin d'évaluer leur efficacité potentielle dans la réalité. Cette revue portera dans un premier temps sur les éléments de base du

PCA, afin de vérifier leur conformité aux objectifs de continuité, aux attentes de la Direction Générale et à la règlementation en vigueur. Ensuite, une revue approfondie analysera le contenu, les rôles et responsabilités, de l'articulation globale… et en validera la pertinence théorique. Ces exercices peuvent être assez révélateurs.
La seconde phase du test consistera en des exercices de simulation, avec la mise en œuvre de scénarios. Des tests unitaires sont menés sur les métiers individuellement et le PSI, ainsi qu'un test étendu portant sur le déclenchement et le pilotage du PCA, pour valider l'efficacité de la gestion de crise. Enfin, un test complet portera sur l'ensemble du PCA en un scénario, qui est nécessaire pour valider l'articulation globale de tous les dispositifs entre eux, et les aspects de sécurité. Il est préférable de tester séparément chaque composante du PCA avant d'effectuer un test global. En effet, un test global de grande envergure risque de se transformer en démonstration, perdant de vue l'objectif initial de détecter les points à améliorer pour perfectionner le PCA. En outre, il est pertinent de débuter la phase de test avec les entités les plus matures. Une simulation peut également porter sur une entité de l'organisation, comme une filiale par exemple.
La troisième phase de test consistera à tester les partenaires de secours et les solutions alternatives (site de repli et SI parallèles notamment), à travers une bascule contrôlée, toujours sur la base d'un scénario. La planification de cet exercice doit être particulièrement minutieuse car elle doit veiller à ne pas perturber le fonctionnement de l'organisation outre mesure.
A un niveau intermédiaire, il est possible d'effectuer l'exercice complet ou des parties de l'exercice sur des environnements qui ne se trouvent pas en production. Enfin, au niveau le plus représentatif, l'exercice est réalisé en production.

La difficulté réside dans la mise en place d'une simulation d'indisponibilité de l'environnement normal de travail qui représente les conditions réelles de la survenance d'une crise. Le scénario de simulation doit être élaboré en collaboration avec des acteurs opérationnels afin qu'ils soient acceptés par les équipes, et être dosé. Le caractère probant du champ couvert par le test ne doit pas être contestable. Un nom de code est donné à l'exercice afin de ne pas confondre exercice et réalité. Une cellule d'animation des tests est formée pour dérouler les scénarios conçus. Elle se chargera notamment de tenir le journal de bord du test. Des observateurs suivent le déroulement du test et peuvent le ralentir voire l'interrompre si ils constatent que les acteurs sont dépassés. Ces exercices insuffisamment cadrés, peuvent présenter des risques de dérapage.

Il est parfois difficile de motiver le personnel autour du test du PCA. En effet, la continuité d'activité va de pair avec des catastrophes importantes, que les employés ne veulent pas envisager. Par ailleurs, un test global du PCA est très transverse, il implique et perturbe toute l'organisation. Il devra donc être réalisé au moment opportun, par exemple lors d'une période calme de l'activité de l'organisation, afin de limiter les perturbations induites.
La planification du test du PCA comporte un important volet de formation et d'information de l'ensemble du personnel, et en particulier les employés directement impliqués dans le test. Elle doit intégrer la réalisation d'un test avec les partenaires et nécessite donc une coordination avec eux. Un programme précis doit être formalisé et communiqué en amont. La réalisation d'un test « surprise » sans en informer préalablement les collaborateurs peut être envisagée pour tester la réactivité de l'organisation, mais présente de sérieux risques de dérapages.

Le test du PCA peut s'appuyer sur le concours d'un intervenant extérieur (cabinet par exemple), ce qui présente l'intérêt d'obtenir des conseils méthodologiques, la possibilité d'être vindicatif à l'encontre d'un membre de la Direction Générale lorsque très peu de personnes en interne peuvent le faire, une perception différente du débriefing, ou encore une ouverture sur d'autres pratiques.

b) Test des PCA et PRA des métiers et fonctions supports

Les tests des PCA et PRA des métiers sont à prévoir spécifiquement en fonction des activités critiques de l'organisation. L'aspect de réactivité, d'information et mobilisation des acteurs dès lors que la situation de crise est déclarée devra cependant être évalué systématiquement.
En ce qui concerne les PCA et PRA des fonctions support, il est notamment essentiel de valider par un test l'efficacité des Moyens Généraux et Techniques, avec la fourniture d'énergie et fluides, dont vont dépendre l'ensemble des PCA métiers. Par exemple, une coupure de l'alimentation électrique permet de mesurer l'efficacité et la réactivité des groupes électrogènes.
Certains tests peuvent intervenir en dehors de l'éventuel site de repli.

c) Test du PSI

Le test du PSI consistera à simuler l'indisponibilité de l'environnement normal informatique, et à vérifier le maintien des systèmes et applications critiques, et de l'accès aux bases de données critiques. Le délai d'interruption et les données perdues seront mesurés, afin de s'assurer qu'ils répondent aux objectifs de DMIA et PMDT du PCA. La sécurité des SI sera par ailleurs testée, par exemple avec des tentatives d'intrusion dans le système pendant la situation de crise simulée.
En raison de la dimension très transverse du PSI, les acteurs métiers et le personnel de la continuité d'activité doivent être au courant et impliqués dans les tests et leurs résultats. En outre, les bonnes pratiques préconisent l'évaluation des résultats du test par un observateur externe à la DSI pour davantage d'objectivité.

d) Test du PCA global et de la gestion de crise

Le test des dimensions transverses telles que la gestion de crise, sécurité et la logistique de crise (site de repli notamment) ne peut intervenir que dans le cadre d'un test étendu voire global, et aura donc lieu après le test des autres composantes du PCA.
Le test du site de repli est essentiel. Son fonctionnement, son accessibilité et le matériel et outils mis à disposition sont vérifiées en déplaçant tout ou partie des opérationnels dans le cadre d'un scénario. Avec les moyens dont ils disposent, et dans un mode dégradé, les salariés doivent être en mesure d'assurer le niveau de service minimum défini dans la stratégie de continuité.
La gestion de la communication de crise, réalisée par la cellule de crise, devra impérativement être testée. Les parties prenantes externes (communication avec les clients, médias…) comme internes peuvent être simulées pour un test indépendant et pour se prémunir d'éventuels dérapages du test, notamment médiatiques.
En ce qui concerne la fonction de surveillance assurée par la cellule de crise, la pertinence des dispositifs prévus peut être revue et évaluée, mais un test pratique ne peut pas être simulé. L'identification des dysfonctionnements ne pourra se faire que dans le cadre d'un retour d'expérience suite à une crise, dont la détection aurait été défaillante.

e) Test impliquant les partenaires externes

Des tests et exercices avec les partenaires doivent être prévus, et un audit préconisé en cas de doute. En cas de défaillance du prestataire, il faut engager un processus d'amélioration avec les Directions de l'entreprise concernée. Il est demandé au sous-traitant de se mettre en situation de répondre au besoin, envisagé de réviser le contrat, son annulation ou la recherche d'un nouveau partenaire.

f) Débriefing et retour d'expérience

La réalisation du premier test technique du PCA est documentée dans un journal de bord du test qui garantit la traçabilité et constitue un élément de preuve pour les instances de tutelles.
Le test doit donner lieu à un débriefing et un retour d'expérience menant à l'amélioration du dispositif. Les dysfonctionnements et les axes d'amélioration sont identifiés par la cellule de crise, puis les organes de gouvernance élaboreront les recommandations correspondantes, qui seront déclinées en plan d'actions par les responsables opérationnels des dispositifs correspondants (PCA métiers et fonctions supports, PSI, cellule de crise) et le RPCA pour les aspects transverses.
Le Comité de Pilotage du PCA validera ces plans d'actions et en suivra la réalisation. Ces éléments font l'objet d'un reporting auprès de la Direction Générale et d'une communication interne et externe.

L'engagement de la Direction Générale se manifestera via un "sponsoring" du test, puis le remerciement de la mobilisation du personnel, la présentation des résultats du test et les améliorations qui en découlent. C'est également elle qui fera un retour sur la réalisation du test auprès du Conseil d'Administration.

Lorsque l'ensemble des composantes du PCA ont été testées, que ce test a remporté un succès satisfaisant, que les améliorations préconisées ont été suivies, cela marque l'achèvement du projet PCA. Le RPCA déclare donc le PCA opérationnel et son passage en phase de maintien en condition opérationnelle.

1.3.3 La maintenance du PCA

Le passage en étape de maintenance du PCA représente le moment où le projet est terminé. Celle-ci ne découle pas de fait, elle doit être déclarée par le RPCA. Le PCA est désormais opérationnel, et constitue un processus de l'organisation à part entière. Il entre dans une phase de maintenance et de mise à jour permanente, assortie de tests réguliers. Cette phase n'est pas seulement l'aboutissement du projet PCA, elle sert des objectifs spécifiques et doit répondre à certaines exigences. L'objectif est de maintenir le PCA en condition opérationnelle en permanence, et d'éviter son obsolescence. Elle sert également des problématiques d'amélioration continue du dispositif.
Les modalités du maintien en condition opérationnelle du PCA sont définies et formalisées dans le PMCO, Plan de Maintien en Condition Opérationnelle, par les organes de gouvernance du PCA, et validées par la Direction Générale, notamment en ce qui concerne les budgets et moyens et l'organisation des tests. Ce plan est généralement pluriannuel, mais révisé chaque année, notamment en ce qui concerne l'allocation de ressources. L'engagement de la Direction Générale demeure essentiel, afin de conserver la mobilisation et la sensibilisation du personnel autour de la problématique de continuité d'activité.
Un budget annuel doit donc être alloué à la maintenance du PCA de l'organisation.

Si le projet PCA (conception et déploiement) était appuyé sur des prestataires et consultants externes de manière importante, la maintenance du PCA peut en être complexifiée. En effet, les connaissances nécessaires peuvent ne pas être disponibles en interne. Il est donc essentiel d'avoir à l'esprit la phase de maintenance dès le départ du projet, afin de s'assurer la possession des éléments nécessaires.

La première année de maintenance du PCA est critique, car c'est au cours de cette année que les dispositifs de continuité vont s'intégrer dans les procédures et modes opératoires quotidiens, et que la continuité d'activité va s'inscrire dans la culture de l'organisation.

1.3.3.1 Veille des évolutions contextuelles

L'environnement dans lequel évolue l'organisation est amené à évoluer, et cela a indubitablement des conséquences sur le PCA. Une veille des éléments contextuels doit donc être réalisée au moins une fois par an, de laquelle découlera la mise à jour des dispositifs de continuité d'activité.

a) <u>Facteurs d'évolution</u>

Règlementation et normes

Dans le cas où le PCA d'une organisation répond à des exigences règlementaires ou normatives, les évolutions de ces référentiels doivent être intégrées dans le PCA.

Stratégie de l'organisation

La stratégie globale de l'organisation impactant la stratégie de continuité d'activité, ces évolutions doivent être intégrées dans la mise à jour du PCA. Il s'agira notamment de recenser les modifications

des objectifs de la Direction Générale et à travers ceux-ci les directives du Conseil d'Administration, l'éventuel repositionnement des activités et des moyens, les réorganisations, fusions, acquisitions ou cessions intervenues depuis la dernière mise à jour du PCA. Les évolutions du SI impacteront parallèlement le PSI.

Marché

Les changements intervenus dans la position de l'organisation sur son marché, tels que l'évolution des parts de marché, sont également à identifier et à intégrer dans la mise à jour de la continuité d'activité.

Partenaires externes

Les évolutions liées aux partenaires externes impactent également la continuité d'activité. Cela concerne notamment les exigences des parties prenantes (clients, instances de tutelle…), les éventuels changements de partenaires, en particulier les prestataires de secours, entrainant la nécessaire mise en place de la démarche avec les nouveaux partenaires. Il faudra également mettre à jour les dispositions prévues avec les partenaires avec qui les contrats sont maintenus, et en particulier les prestataires de secours, en fonction des évolutions qu'ils ont eux-mêmes subis.

Changement de personnel

Les acteurs identifiés dans les procédures de continuité d'activité sont amenés à être modifiés en fonction des mouvements de personnels (arrivées, départs, mutations…), et une mise à jour des procédures s'avérera incontournable.

b) Mise à jour des cartographies des processus et des risques

L'intégration des évolutions de l'organisation dans le plan de continuité passe essentiellement par la mise à jour des cartographies des processus et des risques, en fonction des éléments précédemment identifiés.

c) Mise à jour des analyses d'impact et de la stratégie de continuité

La maintenance du PCA doit contenir une nouvelle analyse d'impact, permettant de mettre à jour celle réalisée lors de la conception du PCA. Celle-ci intégrera les modifications appliquées aux cartographies des processus et des risques, mais également les risques qui sont toujours d'actualité dont les impacts peuvent tout de même avoir évolué. Cette mise à jour peut conduire à une évolution des activités critiques initialement identifiées et du niveau de cette criticité, et donc de la stratégie et des objectifs de continuité. Le PCA dans son ensemble doit ensuite y être adapté.

1.3.3.2 Tests réguliers du PCA

Le maintien en condition opérationnelle du PCA nécessite de le tester régulièrement, une bonne pratique consistant à le faire au moins une fois par an. Ces tests annuels sont effectués en suivant les mêmes modalités de test que le premier test technique du PCA.
Ils sont programmés dans un programme pluriannuel, qui précise la fréquence et la stratégie de test. Ce plan tient compte des moyens alloués à la réalisation de ces tests, et à leur caractère progressif. Il est donc réactualisé chaque année en fonction du budget dédié à la maintenance du PCA.
Les tests réguliers portent sur toutes les composantes du PCA afin de valider qu'elles sont toujours efficaces et pertinentes, et apporter les éventuelles corrections et mises à jour qui s'avéreraient nécessaires.
Au fur et à mesure des années et des tests, on va chercher à augmenter la complexité du test, à couvrir de plus en plus de scénarios et à se rapprocher au maximum des conditions d'une activation réelle. La réalisation des tests elle-même fait donc l'objet d'une mise à jour et d'une amélioration. Au fil des tests, une certaine standardisation des protocoles de secours et des réactions se met en place, ce qui est utile pour installer les bons réflexes chez les collaborateurs, mais ne doit pas freiner l'innovation et une certaine souplesse nécessaire face à l'imprévu.

La réalisation et les résultats de chaque test sont consignés dans un journal de bord et donnent lieu à un retour d'expérience et à des améliorations tout comme à la suite du premier test. Le RPCA est responsable de cette maintenance et en rend compte. Tous les documents sont datés et signés et constituent des éléments de preuve vis-à-vis de l'audit interne et des instances de tutelle.

1.3.3.3 Mise à jour des évaluations financières

Le PCA devant être considéré avec un coût en constante évolution, il est nécessaire de réactualiser régulièrement le chiffrage des PCA.
Cela doit permettre la remise en question des PCA en fonction de l'évolution des estimations, à travers un nouveau rapprochement du coût du PCA avec le coût d'une interruption de l'activité, et valider la pertinence des solutions retenues, ou apporter les modifications correspondantes.

1.3.3.4 Mise à jour des procédures

Enfin, l'ensemble des procédures du PCA, incluant celles du PRA, PSI, de la Gestion de Crise et les PCA et PRA métiers et fonctions supports, seront mises à jour, de manière refléter l'évolution de l'entreprise et de la stratégie de continuité. Ces mises à jour doivent suivre l'évolution des procédures opérationnelles. Un outil de suivi simple et efficace devrait être mis en place pour garantir la mise à jour des procédures PCA.
Les mallettes de crise devront également être réajustées.

Le maintien en condition opérationnelle du PCA, et notamment sa mise à jour est une phase essentielle qui ne doit pas être négligée, puisqu'un plan obsolète n'est d'aucune utilité lors d'une crise et est même susceptible d'entraîner d'autres dommages (notamment dans le PSI, avec la bascule d'un mauvais serveur par exemple, pouvant entraîner la perte de données importantes, voire critiques).

1.4 Spécificités sectorielles de mise en place d'un PCA et d'une gestion de crise

1.4.1 Secteur bancaire

Comme il a été évoqué précédemment, le secteur bancaire est particulièrement règlementé, notamment sur ce qui a trait à sa continuité d'activité et les dispositifs mis en place pour l'assurer.
Cette règlementation conditionne naturellement les activités critiques qui sont spécifiques au secteur bancaire, et pour lesquelles les établissements se doivent de mettre en place des dispositifs visant à assurer un niveau de service minimum en toutes circonstances.
D'une manière générale, l'organisation et le pilotage de la démarche de continuité d'activité constitue en elle-même une activité critique, et une attention particulière doit être accordée à la désignation des responsables PCA et PSI, ainsi qu'à la définition de leurs rôles, responsabilités, pouvoirs et délégations de pouvoirs. C'est également à travers cette activité qu'est prévu le reporting relatif à la continuité d'activité.
Les contrôles permanents et l'assurance de la conformité règlementaire constituent également une activité essentielle dans le secteur bancaire, qu'il est nécessaire de garantir en situation de crise. Ainsi, ces contrôles s'étendent à la démarche PCA et sont intégrés à la fois au plan de contrôle et aux PCA.
D'un point de vue plus opérationnel, ce sont les systèmes d'information qui constituent l'élément central des dispositifs de continuité. En effet, c'est sur eux que repose le cœur de l'activité bancaire, et leur interruption aurait des conséquences dramatiques pour l'activité. Il est donc essentiel d'établie et documenter un PSI efficace, pertinent et opérationnel, qui soit complet, validé de manière appropriée et fasse l'objet d'un maintien en condition opérationnelle. Il doit notamment inclure des dispositifs de protection physique du matériel, ainsi qu'un plan de sauvegarde et protection des données sensibles et confidentielles, une contractualisation sans faille avec les prestataires de secours et une bonne identification des données et applications critiques.
La démarche de continuité d'activité d'un établissement bancaire s'appuie également sur un plan de repli utilisateurs, qu'il est important de prévoir et maintenir en condition opérationnelle. Ce plan de repli prévoit notamment un site de repli, équipé du matériel (notamment informatique) nécessaire pour assurer la continuité des activités critiques ainsi que des données et applicatifs critiques. La contractualisation avec les prestataires de secours est ici essentielle.
Enfin, la continuité d'activité doit s'étendre aux prestataires de services essentiels, en visant à s'assurer de leur continuité d'activité et de leur conformité aux dispositions règlementaires.

1.4.2 Secteur de la santé publique

En parallèle des éléments de continuité d'activité génériques, il existe des dispositifs de continuité d'activité et de gestion de crise qui sont spécifiques à un établissement de santé.

1.4.2.1 Continuité d'activité

Les établissements de santé sont caractérisés par un rôle sanitaire et social de secours et d'assistance en cas de survenance d'un sinistre externe provoquant un afflux de victimes. Cela, couplé avec leur propre continuité d'activité interne, pose une certaine dualité dans la démarche. Ils doivent en effet prévoir une continuité d'activité pour pallier aux risques d'incidents internes, mais également d'être

en mesure de s'intégrer dans une démarche plus globale en tant qu'acteur de secours d'une crise externe.
En termes de continuité d'activité interne, quatre activités sont identifiées comme critiques et nécessitent donc le maintien en permanence d'un niveau de service minimum :

- Le fonctionnement du matériel biomédical
- Les services techniques
- Les systèmes d'informations et télécoms
- Les approvisionnements

Il est donc indispensable de prévoir des dispositifs de continuité d'activité relatifs à ces processus en cas de survenance d'un incident venant compromettre l'environnement normal de travail.
Par ailleurs, une continuité d'activité externe doit être conçue, en prévoyant l'intégration de l'établissement dans un dispositif plus global, régi par des éléments règlementaires relatifs à la gestion de crise.

1.4.2.2 Alerte et Gestion de Crise

Les bonnes pratiques de gestion de crise dans un établissement de santé recommandent la mise en place de plusieurs dispositifs spécifiques.
Tout d'abord, une veille et une analyse quotidienne des indicateurs d'activité quotidienne disponibles est réalisée par une cellule de veille, qui formalise son travail dans des tableaux de bord afin de détecter et d'anticiper la survenance d'une crise. Elle se charge également de communiquer des informations aux serveurs régionaux qui centralisent les indicateurs de l'ensemble des établissements de santé pour une gestion globale.
Lors de la détection d'un incident, l'alerte est déclenchée par la cellule de veille et une cellule de crise réduite est mobilisée, chargée essentiellement d'évaluer la situation et d'essayer de la traiter si la gravité est limitée. S'il s'agit d'un sinistre grave, c'est l'escalade et la cellule de crise complète est mobilisée, et le Directeur de l'établissement peut aller jusqu'à déclencher le plan d'urgence interne, le plan blanc.
Dans le cas de la survenance d'une crise globale provoquant un afflux massif de victimes et nécessitant la mobilisation de plusieurs établissements, l'établissement de santé considéré doit être en mesure de s'intégrer dans les plans d'urgences globaux que sont le plan blanc élargi, les plans rouges, les plans de secours ORSEC, les plans particuliers d'intervention, les plans de secours spécialisés, les plans gouvernementaux "pirates" ou les plans sanitaires spécifiques.
L'établissement de santé doit également s'articuler avec une organisation sur le terrain, telle que le SAMU-SMUR et la cellule d'urgences médico-psychologiques.

1.4.3 Secteur alimentaire

Le secteur alimentaire dispose également de spécificités sectorielles qui permettent d'identifier les activités critiques propres à ce secteur d'activité, pour lesquelles des dispositifs de continuité d'activité sont nécessaires.
Ainsi, la sécurité des infrastructures et sites de production constitue l'une de ces activités critiques, puisqu'un site de production de repli équipé et opérationnel est nécessaire dans le cadre du déploiement des dispositifs de continuité d'activité, qu'il s'agisse d'un site spécifiquement dédié aux

situations de crise, ou la capacité d'un autre site de production à prendre le relai et assurer un niveau de service minimum.
Une attention particulière est également accordée aux équipements lourds de production dans le cadre d'une démarche de continuité d'activité, en particulier en ce qui concerne la garantie de la sécurité, la maintenance des équipements, et la garantie de la continuité d'activité au travers d'équipements de secours opérationnels prévus.
La continuité d'activité d'une organisation appartenant au secteur alimentaire est en outre conditionnée par la continuité de la chaîne de production. En effet, la production alimentaire est généralement subdivisée en différentes phases de production, localisées sur des sites différents et assurées par des acteurs différents. Il est donc nécessaire de s'assurer de la continuité d'activité à chacune de ces étapes ainsi que des relations entre les différents acteurs. Des solutions palliatives en cas de défaillance de l'un des acteurs sont également à prévoir par les autres acteurs de la chaîne.
La sécurité alimentaire constitue une activité critique de ce secteur d'activité, de par les conséquences lourdes qui découleraient d'une défaillance de cette sécurité. Les nombreuses normes d'hygiène et de sécurité qui s'y attachent doivent être respectées, et la qualité et la conformité du conditionnement doit être garantie en toutes circonstances. Le transport et la conservation des aliments sont également à surveiller, notamment en ce qui concerne le maintien de la chaîne du froid.
Enfin, la continuité de l'alimentation en énergie est également une activité critique pour le secteur alimentaire, puisqu'elle conditionne le déploiement des dispositifs de continuité. Des dispositifs pertinents doivent être prévus et opérants pour assurer cette continuité d'alimentation.

1.4.4 Secteur de l'énergie

Le secteur de l'énergie, de par la règlementation qui l'encadre, a des obligations de service public. La continuité de la fourniture d'un service de distribution d'énergie nécessite le maintien du fonctionnement du réseau en toutes circonstances car beaucoup d'autres secteurs d'activité en dépendent.
D'autre part, la dimension sécurité des personnes est très importante dans ce secteur, car la survenance de sinistres, bien que rare, a des conséquences dramatiques (explosions de gaz, asphyxies, morts et blessés,…etc.).
Aussi, la maitrise des risques dans ce secteur doit être totale, et cela sous-entend une anticipation de la survenance des sinistres et des mesures solides de gestion de crise, en particulier la protection du personnel et des utilisateurs.
Pour ce faire, les volets critiques qu'il est nécessaire de surveiller et de maintenir (dans le cas particulier du gaz par exemple) sont la sécurité des réseaux de distribution, la continuité de l'approvisionnement, la surveillance des espaces de stockage du gaz, la sécurité des consommateurs et du personnel, la pertinence et la disponibilité des ressources humaines, ainsi que la continuité de fonctionnement des systèmes d'information industriels.

1.4.5 Secteur des transports

Le secteur d'activité des transports répond à des exigences de service public qui définissent le niveau de service minimum qui doit être assuré en toutes circonstances.

Au-delà des aspects génériques de continuité d'activité, ce service minimum règlementaire conditionne en conséquence les activités spécifiques les plus critiques des organisations responsables d'assurer ces services.
Ces activités critiques vont concerner notamment les aspects de sûreté et de sécurité des voyageurs, eu égard à la protection contre le terrorisme et les incendies notamment, y compris en période de crise. Dans la mesure où il s'agit d'infrastructures destinées à recevoir du public, ces aspects sont particulièrement importants.
Les services techniques, notamment d'alimentation en énergie et en fluides, sont également essentiels. Dans le cas de l'aviation civile, cela se manifeste par exemple dans la continuité de l'alimentation électrique des installations de guidage des aéronefs, le balisage des pistes et la tour de contrôle.
L'information aux voyageurs figure également parmi les obligations de service minimum des transports, ce qui en fait une activité critique pour laquelle il est nécessaire de prévoir une continuité d'activité.
En outre, la viabilité hivernale est une activité critique commune à tous les types de transports, nécessitant la mise en place de dispositifs de continuité d'activité spécifiques.
Par ailleurs, dans le cas particulier de l'aviation civile, le péril animalier et le balisage des pistes sont également critiques.

La mise en place de la gestion de crise dans une organisation relevant du secteur d'activité des transports doit inclure l'obligation d'information des autorités compétentes lors de la survenance d'un incident, prévisible ou non. Elle prévoit par ailleurs le secours, l'accueil et l'information au public, notamment la gestion des appels en cas de sinistre grave impliquant des victimes.

Au vu de la règlementation qui encadre la mise en place de ces différents dispositifs, les organisations doivent rendre compte de leur capacité à répondre aux exigences.

1.4.6 Secteur des télécommunications

Le secteur des télécommunications, de par la règlementation qui l'encadre, a des obligations de service public, notamment le service universel, dont il doit assurer la continuité.
Ces éléments viennent conditionner les activités critiques des organisations de ce secteur, activités pour lesquelles il sera nécessaire de mettre en place des dispositifs de continuité d'activité.
Ainsi, la continuité de la fourniture d'un service téléphonique et de services complémentaires de communications électroniques nécessite le maintien du fonctionnement et de l'accessibilité du réseau en toutes circonstances, en particulier dans le cas de la survenance d'un sinistre.
Pour ce faire, les activités critiques qu'il est nécessaire de maintenir sont essentiellement ses infrastructures, le système d'information et la continuité d'alimentation en énergie, ainsi que la continuité des approvisionnements clés, tels que les puces électroniques. La disponibilité du personnel est également une nécessité essentielle à la continuité d'activité.

1.5 Les outils

Les outils spécifiques à la continuité d'activité et la gestion de crise ne font pas légion dans les organisations, en particulier en ce qui concerne les outils informatiques. Les logiciels PCA qui existent constituent essentiellement une aide à la documentation du PCA et au stockage des documents, et non à sa construction. Ils sont par ailleurs souvent trop standardisés pour être réellement utiles aux spécificités d'une organisation. Certaines organisations vont développer en interne des outils pour supporter leur démarche de continuité d'activité et de gestion de crise, mais ce type de pratiques reste marginal.

Il existe néanmoins des outils de type SIMCA (Système d'Information du Management de la Continuité d'Activité), visant à mettre à jour en temps réel toutes les informations vitales de l'entreprise, et éventuellement son réseau de partenaires proches. Un tel outil peut s'avérer utile dans le cadre de la maintenance en condition opérationnelle du PCA, mais peut engendrer des coûts et une gestion superflus au vu de la plus-value qu'il apporte.
L'outil informatique peut également être utilisé pour l'évaluation des dégâts et la gestion et répartitions des responsabilités et tâches en situation de crise.
Des outils peuvent également être développés dans le cadre de la veille permanente, qui vise à détecter et anticiper les incidents, en mettant en place des applicatifs de suivi des indicateurs d'activité clés.
Aux Etats-Unis, il existe le NIMS (National Incident Management System), commun aux entreprises et aux administrations. En Europe, un tel dispositif n'existe pas.

En dehors des considérations informatiques, la démarche PCA s'appuie sur des indicateurs, des tableaux de bord, des référentiels, des cartographies et des plans d'actions, ainsi que la base d'incidents de l'organisation. Ces outils sont mis en place lors de la conception du PCA, et utilisés tout au long de la démarche. Il s'agit toutefois d'outils assez génériques, qui peuvent être adaptés à tous types de projets et démarches, dont la continuité d'activité et la gestion de crise.
Pour le cas particulier de la gestion de crise, pourront être mis en place des tableaux "occurrence, gravité, probabilité" visant à évaluer les incidents dans le cadre d'une veille, et détecter l'éventuelle nécessité d'enclencher une procédure d'alerte.
Les outils déployés dans le cadre du PCA doivent être en adéquation avec ceux des autres dispositifs de maîtrise des risques, en particulier le Management des Risques et le Contrôle Interne.

Synthèse de la première partie

- Un PCA est un dispositif de Management des Risques visant à assurer la continuité des activités critiques d'une organisation à un niveau de service minimum et dans un mode dégradé, dans l'éventualité de la survenance d'un sinistre grave. Il ne vise pas à empêcher la survenance de ce sinistre, mais à protéger l'organisation contre ses impacts, et notamment l'interruption des activités.
- Il se compose de plusieurs PCA et PRA métiers pour les activités critiques, qui s'appuient sur des PCA et des PRA fonctions supports, un PSI, une gestion de crise et une organisation globale du PCA qui coordonne ces éléments.
- La mise en place de ce dispositif de continuité d'activité est règlementé pour les secteurs d'activités critiques, dits vitaux (bancaire, santé publique, alimentation, énergie, transport, télécommunications) et intéresse les différentes parties prenantes d'une organisation.
- La mise en place d'un PCA dans une organisation passe par un projet PCA, prévoyant la conception et le déploiement du dispositif, puis son maintien en condition opérationnelle sur la durée.
- Les principaux points de contrôle clés de la démarche PCA sont :
    - La formalisation de cartographies des processus et des risques
    - L'analyse de l'impact des risques
    - La sélection des activités critiques, la définition de leur niveau de service minimum et des objectifs de continuité (DMIA et PMDT notamment)
    - L'élaboration des solutions de secours pour les métiers et fonctions support, ainsi que le PSI, de manière à répondre aux objectifs de continuité, aux attentes de la DG et aux obligations règlementaires
    - La vérification de la faisabilité et la pertinence de ces solutions
    - Un déploiement des ressources et moyens adapté, notamment à travers une coordination globale de la démarche, intégrant les problématiques de sécurité et de logistique (site de repli notamment)
    - La sensibilisation des collaborateurs et la formation des acteurs
    - La mise en place d'une gestion de crise, assurant notamment une veille pour détecter et anticiper la survenance des sinistres
    - Le test du PCA permettant de vérifier qu'il est opérant
    - Le maintien en condition opérationnelle et la mise à jour du PCA
- Les bonnes pratiques recommandent également de prêter attention à :
    - L'identification des acteurs de la démarche et leurs rôles, responsabilités et pouvoirs
    - Une implication forte de la Direction Générale
    - L'intégration de la démarche à la culture de l'organisation, et l'adhésion du personnel
    - Une stricte documentation du PCA
    - Une politique de communication interne et externe soignée
    - L'implication des principaux partenaires externes dans la démarche
- Bon nombre de ces éléments concernent toutes les organisations, indépendamment de leur secteur d'activité. Les spécificités sectorielles conditionnent essentiellement l'identification des activités critiques pour lesquelles il est nécessaire de prévoir une continuité des activités, à la fois à travers les exigences règlementaires concernées, mais aussi en conséquence des enjeux et risques spécifiques du secteur d'activité.

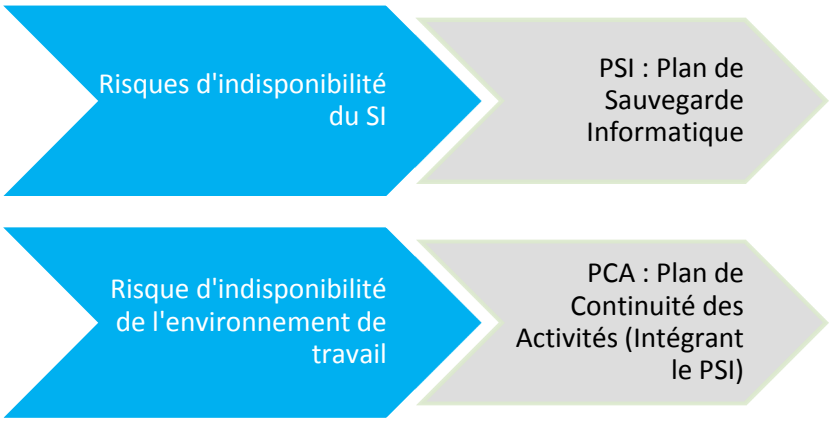
2. Les risques associés aux plans de continuité d'activité

2.1 Risques majeurs d'indisponibilité de l'environnement de travail (Génériques)

Le PCA d'une organisation vise à préserver celle-ci des impacts des risques majeurs auxquels elle est vulnérable, sinistres de grande ampleur, susceptibles de la priver de son environnement normal de travail, et même de causer sa disparition. Ceux-ci sont de plus en plus nombreux, imprévisibles et de grande envergure. Les effets qui en découlent sont dévastateurs et souvent ces dernières ne s'en remettent pas.

Ces grands sinistres constituent des risques "causes", qu'il est nécessaire d'identifier afin d'y être préparé. C'est cependant aux impacts potentiels de leur occurrence que les organisations sont réellement sensibles, et contre lesquels elles vont chercher à se prémunir à travers la mise en place d'un PCA. Ces impacts potentiels constituent les risques "conséquences", qui seront également identifiés.

L'ensemble de ces éléments permet de construire la cartographie des risques PCA d'une organisation, où les risques seront évalués en termes de risque d'occurrence et de puissance de l'impact. L'identification de ces risques particulièrement importante, du fait que des risques ambigus ou mal définis sont d'autant plus générateurs d'anxiété collective qu'ils donnent l'impression de ne pas être maîtrisés. Seront identifiés ci-après les risques génériques communs à tous types d'organisation, indépendamment de leur taille ou de leur secteur d'activité. Lorsque le PCA d'une organisation visera à mettre en place des dispositifs pour la préserver des impacts des sinistres, les ramener à un niveau de risques résiduels acceptables et maintenir la continuité de ses activités critiques, l'audit de ce PCA cherchera à vérifier que l'ensemble de ces risques « impacts » sont couverts.



Les risques "causes" peuvent être d'origines multiples, et sont classifiés selon différentes typologies.

2.1.1 Sinistres naturels

2.1.1.1 Risques "causes"

Les sinistres naturels sont les catastrophes naturelles, telles que les tsunamis, crues centennales, tremblements de terre, intempéries violentes, changements climatiques, incendies naturels…
Les avancées scientifiques et technologiques rendent ces évènements plus faciles à prévoir et anticiper, permettent éventuellement d'en diminuer l'intensité, mais leur évitement est difficilement concevable.

2.1.1.2 Risques "conséquences"

Les catastrophes naturelles peuvent entraîner la destruction des bâtiments et infrastructures (en particulier le SI) de l'organisation, ou tout du moins les endommager. Elles peuvent également provoquer une indisponibilité des réseaux, télécommunications ou moyens de transport sur lesquels s'appuie l'activité de l'organisation. Une autre conséquence possible est la défaillance des partenaires, fournisseurs et sous-traitants, venant perturber les opérations. Il faut également envisager les potentiels dégâts humains, entraînant une indisponibilité de tout ou partie du personnel de l'organisation.

2.1.2 Sinistres technologiques

2.1.2.1 Risques "causes"

Les sinistres technologiques sont les incidents de type accident industriel ou panne technique, pouvant se présenter sous la forme d'un incendie ou de l'explosion d'un site, d'un accident des transports, ou encore d'un produit ou d'un équipement défectueux, de défaillance d'infrastructures. Ils peuvent par ailleurs résulter de la simple réalisation de travaux publics. Les virus informatiques constituent également un risque technologique.
La probabilité de survenance d'un sinistre technologique impactant une organisation est renforcée si celle-ci est localisée à proximité d'un site sensible.
La directive européenne n°96/82/CE, également dite "Seveso" impose aux Etats membres de l'Union Européenne de recenser l'ensemble des sites à risques du territoire, dans un objectif de prévention des risques industriels majeurs. Les sites identifiés sont tenus de mettre en place des plans de secours adaptés et à être capable de s'intégrer dans un plan de secours plus global en cas de sinistre.

2.1.2.2 Risques "conséquences"

A l'instar des catastrophes naturelles, les sinistres technologiques peuvent être préjudiciables pour l'intégrité des bâtiments et infrastructures, du personnel et des supports externes sur lesquels repose l'activité de l'organisation, tels que les télécommunications, réseaux et transports.
A ces risques d'impact viennent s'ajouter les risques juridiques et d'image dans le cas où la cause de survenance du sinistre relève de la responsabilité de l'organisation, où une défaillance de son Contrôle Interne aurait conduit à l'incident. La problématique de continuité d'activité se manifesterait alors dans la recherche de la sauvegarde de l'organisation suite à l'incident, par

opposition à la recherche de son évitement qui est une problématique de Contrôle Interne. Le risque d'image peut entraîner un risque commercial de perte de clientèle et de parts de marché.

2.1.3 Sinistres sociaux, économiques et politiques

2.1.3.1 Risques "causes"

Les sinistres sociaux, économiques et politiques peuvent se présenter sous des formes relativement variées, qu'il s'agisse de la survenance d'une guerre ou d'attentats terroristes, ou bien d'une crise économique entraînant l'instabilité des marchés. Ils peuvent également se manifester sous forme d'occupation des locaux, de grèves ou de groupes de pression. Enfin, la possibilité de malveillance humaine n'est pas à omettre, et le vandalisme, les actes délictueux ou le sabotage sont également à envisager.

2.1.3.2 Risques "conséquences"

Ce type de sinistre peut résulter en une indisponibilité de tout ou partie du personnel, comme des infrastructures externes nécessaires à l'activité de l'organisation. Une baisse du pouvoir d'achat général peut par ailleurs entraîner une perte importante de clientèle, de Chiffre d'Affaire et de marge de l'organisation. Les objectifs stratégiques de l'organisation peuvent donc ne pas être atteints. Les conflits sociaux pourront impliquer des conséquences juridiques et d'image, et les actifs de l'organisation seront menacés par une guerre, des actes de terrorisme ou de malveillance.

2.1.4 Sinistres sanitaires

2.1.4.1 Risques "causes"

Le risque de pandémie grippale ou d'épidémie est une menace grandissante, avec laquelle les organisations doivent apprendre à composer. Avec la mondialisation et les modifications globales de l'environnement, son occurrence est favorisée.
Un risque sanitaire peut par ailleurs être lié à un incident technologique provoquant une contamination, ou un potentiel acte de bioterrorisme, favorisé et aggravé par les avancées scientifiques en la matière.

2.1.4.2 Risques "conséquences"

Le risque sanitaire, en particulier celui de pandémie grippale peut concerner tous types d'organisation, en ceci qu'il peut les priver de tout ou partie de leurs effectifs. Privées de leur personnel, la continuité des activités est compromise.
Il est difficile de mesurer l'ampleur des conséquences que pourrait entraîner une crise sanitaire, puisque son occurrence n'est pas nécessairement limitée ni dans sa localisation, ni sans sa durée, ni dans son ampleur. Sans qu'elle entraîne nécessairement d'incidences matérielles, sauf accidents induits, elle peut paralyser bon nombre d'activités en conduisant au confinement voire au décès de la population.

2.1.5 Sinistres nucléaires, radiologiques, biologiques et chimiques

2.1.5.1 Risques "causes"

Ce type de sinistres est mis à part en raison de ses caractéristiques particulières.
Risque renforcé par les menaces terroristes, les avancées scientifiques et technologiques en la matière
Risque renforcé par la proximité d'un site à risque
Peut résulter d'une catastrophe naturelle ou d'un accident industriel

2.1.5.2 Risques "conséquences"

Les grands risques "causes" peuvent en outre s'enchaîner en cascade. Ainsi, une catastrophe naturelle ou un accident industriel peuvent entraîner une instabilité des marchés, une manifestation sociale ou une crise sanitaire.
L'interdépendance grandissante des acteurs économiques démultiplie les risques « conséquences » pour une organisation, dans la mesure où tout sinistre impactant un partenaire aura des conséquences sur l'organisation considérée.

L'identification de l'ensemble de ces risques va conduire les organisations à une prise de conscience par la peur, et les pousser à mettre en place une démarche PCA.

2.2 Risques d'impacts liés aux points de contrôle clés de continuité (Génériques)

Les différentes étapes de mise en place du PCA entraînent des risques d'impacts qui découlent potentiellement de la non mise en place des points de contrôle clés qui y sont attachés. Il s'agit de ce type de risques qui sera listé ci-après, déroulés selon chaque étape de mise en place du PCA.

2.2.1 Risques liés à la conception du PCA

2.2.1.1 Préalable

En l'absence d'une bonne communication interne préalablement au démarrage du projet et de la conception du PCA, les salariés ne sont pas sensibilisés à la continuité d'activité. Pour certains d'entre eux, ils peuvent ne pas connaître et comprendre le concept, ils n'en voient pas l'intérêt, ne savent pas à quoi sert ce dispositif. Cela peut conduire à un désintéressement du personnel à la démarche PCA et une absence de leur implication.
Sans implication du personnel, le projet PCA ne peut pas être un succès. Sa conception repose sur la qualité du travail des salariés du début à la fin, sur leur minutie comme sur leur imagination, qui seront de moins bonne qualité s'ils ne sont pas motivés par la démarche.

2.2.1.2 Etape 1 : Constitution de l'équipe PCA

L'équipe PCA regroupe les personnes qui vont porter et faire vivre le projet PCA. Si le choix des personnes qui la composent n'est pas bon, l'organisation peut se retrouver avec des pilotes de son PCA qui ne disposent pas d'une vision suffisamment transverse, et focalisés sur une vision métier, trop réductrice pour mener à bien la démarche. D'une manière générale, si l'équipe PCA se compose de personnels insuffisamment compétents, ne maîtrisant que trop légèrement le sujet, peu motivés, impliqués et disponibles pour le projet, ou ne disposant pas de la position hiérarchique permettant de le porter, la démarche PCA ne sera pas menée de manière optimale, et les dispositifs de continuité peuvent ne pas être opérants.
Ce risque est important si les organes de gouvernance sont dans l'incapacité de prendre les décisions adéquates, si le RPCA ne peut porter le projet et coordonner tous les acteurs, et si le RPSI et les CCA ne savent pas mobiliser leurs équipes sur la démarche.

2.2.1.3 Etape 2 : Définition des activités critiques et de la stratégie de continuité

a) <u>Identification des activités critiques</u>

L'ensemble de la stratégie de continuité repose sur les processus et les risques identifiés. Si celles-ci sont mal élaborées, non exhaustives et incomplètes, ce sera le cas de la démarche dans son ensemble. En effet, l'omission d'un risque ou d'un processus critiques lors de l'établissement de ces cartographies, s'il n'est pas découvert ultérieurement risque de provoquer une faille dans le maillage du PCA, puisqu'aucun besoin en continuité ne sera identifié, et donc aucun dispositif de continuité ne sera prévu pour couvrir ce risque ou ce processus critique.
Par ailleurs, si les cartographies sont incomplètes, notamment en termes de flux entrants et sortants des processus et d'impact des risques, les solutions imaginées pour assurer la continuité du service

minimum des activités critiques par rapport aux risques seront inadaptées, potentiellement inopérantes, et les besoins en ressources et moyens pour déployer ces solutions qui seront identifiées ne correspondront pas à la réalité.
Au-delà du risque de défaillance du dispositif de continuité d'activité de l'organisation, cela peut éventuellement entraîner des surcoûts.

L'absence d'analyse des impacts d'une interruption d'activité empêche l'organisation de se faire une idée réelle des impacts qu'elle encourt vis-à-vis des risques auxquels elle est vulnérable. Sans cette prise de conscience, elle ne saura pas définir efficacement ceux contre lesquels il est essentiel de se prémunir. Ici, c'est donc la pertinence de la stratégie de continuité qui est menacée, et c'est de cette stratégie que découleront l'ensemble des dispositifs de continuité mis en place. Le PCA pourrait alors être complètement inadapté aux besoins réels de l'organisation, ne pas garantir la continuité de ses activités critiques ni la protéger contre les risques les plus dangereux.
Si l'analyse d'impacts n'est pas réalisée correctement, ce sont les DMIA et PMDT qui risquent d'être mal définis, et puisqu'ils conditionnent ensuite les objectifs de continuité, les solutions élaborées par rapport à ces objectifs ne seront peut-être pas totalement opérantes.

Dans le cas où une organisation ne prendrait pas correctement en compte les risques et les besoins en continuité de ses partenaires externes, et notamment les fournisseurs de services essentiels, ainsi que les dispositifs de Contrôle Interne et de continuité d'activité qu'ils ont mis en place, deux dimensions de risques "conséquences" peuvent être envisagées. En effet, soit elle appuiera ses dispositifs PCA sur la certitude de la continuité de fourniture des services externes essentiels alors qu'ils ne sont pas garantis, menaçant alors l'efficacité de sa propre continuité, soit elle partira du principe que ses partenaires ne sont pas fiables et déploiera des dispositifs pour palier à leur défaillance, risquant un doublage des dispositifs avec ceux mis en place par les partenaires et donc un gaspillage des ressources.

Selon la même logique, une absence ou une mauvaise prise en compte des dispositifs de Contrôle Interne déjà existants en interne préalablement à la démarche PCA dans l'organisation peut causer soit une faille non identifiée et donc un risque de défaillance du PCA, soit des doublons de dispositifs internes et un gaspillage de ressources.

Par ailleurs, si toutes les phases de définition de la stratégie ne font pas l'objet d'une consultation et d'une validation par la Direction Générale, et que celle-ci ne les suit pas, la démarche risque de ne pas être légitimée en interne auprès des collaborateurs, réduisant d'autant leur motivation et leur implication dans le projet. Il est également possible que la démarche PCA soit complètement déconnectée des objectifs stratégiques de l'organisation, ne remplissant alors pas son rôle. Un autre point d'attention réside dans le risque que, non consultée et peu impliquée, la Direction Générale renâcle à attribuer ressources et moyens au PCA.

L'absence de prise en compte des obligations règlementaires lors de la conception du PCA présente le risque de non-conformité de celui-ci avec ces obligations, entraînant de potentielles sanctions pour l'organisation, avec des conséquences financières et d'image.
Enfin, cette phase se solde par l'identification des activités critiques et du niveau de criticité de ces activités qui, mal réalisée, conduira très probablement à une stratégie de continuité inadaptée et

donc des dispositifs de continuité ne permettant pas de garantir la continuité et la reprise des activités critiques de l'organisation.

b) Elaboration de la stratégie de continuité

Si les besoins en continuité des métiers ne sont pas ou mal définis, les objectifs de continuité seront inexistants ou inadaptés. Sans connaître le niveau de service minimum qu'il est nécessaire de maintenir ou le DMIA, le PMDT et le délai de reprise, il est difficile pour les opérationnels de prévoir des dispositifs de continuité d'activité qui soient pertinents. Le risque ici est donc d'avoir des dispositifs de continuité inadaptés aux besoins de l'organisation ou inopérants.

L'essentiel du PCA d'une organisation reposant sur les PCA métiers des activités critiques, les autres composantes venant en support à celle-ci, l'élaboration de ces solutions de PCA métiers est réellement le cœur de la conception du dispositif. Une absence ou une mauvaise élaboration de celles-ci rendrait caduque l'ensemble du PCA.

L'absence ou la mauvaise définition des ressources et besoins nécessaires aux solutions risquerait d'engendrer, si elles sont sous-évaluées, une allocation insuffisante empêchant le déploiement de celles-ci et donc une défaillance du PCA ou bien, si elles sont surévaluées, la non-validation de celles-ci par la gouvernance du PCA et la Direction Générale alors qu'elles auraient pu être parfaitement opérantes.

Le PSI venant en support aux PCA métiers, l'éventualité où il n'existerait pas ou ne serait pas performant viendrait priver les opérationnels des outils sur lesquels reposent leurs dispositifs de continuité et rendraient impossible le déploiement de ceux-ci. La continuité des activités critiques de l'organisation ne serait donc pas garantie.
La problématique est assez similaire dans le cas des solutions des PCA services supports, puisqu'elles sont sensées assurer le niveau de service minimum défini par les métiers comme nécessaire au déploiement des PCA métiers.
L'idée peut également être étendue aux dispositifs de continuité des partenaires de l'organisation.

En l'absence d'une organisation globale du PCA, l'organisation encourt le risque d'insécurité du personnel en cas de survenance d'une crise, car la mise en place de cette sécurité ne relève du périmètre d'aucune autre composante du PCA. Il en va de même en ce qui concerne la logistique de crise, et l'organisation se retrouverait ainsi sans site de repli, ou alors un site de repli non opérationnel vers lequel la migration n'est pas prévue ou pas possible.
Par ailleurs, sans coordination globale des ressources (financières, humaines, matérielles) allouées aux différentes composantes, il peut y avoir conflit sur leur répartition ou insuffisance de celles-ci en cas de survenance d'un sinistre, avec la potentielle impossibilité d'enclencher simultanément tous les dispositifs.
En effet, sans organisation globale, la cohérence globale de tous les dispositifs, la circulation des flux et les goulots d'étranglement ne sont pas vérifiés.

Dans le cas particulier des structures complexes, si la problématique de continuité d'activité n'est pas envisagée dans l'ensemble des structures avec une cohérence globale, le groupe considéré s'expose

à un risque de non sécurisation de sa continuité d'activité lorsque les différentes entités qui la composent sont interdépendantes entre elles. En outre, la non mutualisation des moyens entre les différentes entités peut conduire à un gaspillage de ressources.

Enfin, si la dimension préventive du PCA (d'intégration des problématiques de continuité dans les nouveaux projets et de réduction du risque de survenance d'un sinistre) n'est pas correctement maîtrisée et anticipée, la nécessaire mise en place ultérieure de dispositifs de continuité d'activité entraînera des coûts qui auraient pu être réduits voire évités.

c) Validation de l'étape

L'étape de définition des activités critiques et de la stratégie de continuité s'achève idéalement sur une validation de l'ensemble des éléments par la gouvernance du PCA et la Direction Générale. Sans une validation de ce type adéquate, le déploiement du PCA dans son ensemble peut être compromis par la mise en attente du projet ou l'absence d'allocation des ressources et moyens nécessaires.
En outre, si la stratégie de continuité n'est pas certifiée conforme aux exigences règlementaires, même sa stricte application ne prémunira pas l'organisation contre d'éventuelles sanctions de non-conformité.

2.2.1.4 Etape 3 : Etudier et choisir les solutions envisageables

a) Etude de faisabilité et chiffrage des solutions

Sans étudier la faisabilité des solutions de continuité envisagées, l'organisation s'expose au risque qu'il ne soit pas possible de les déployer le moment venu, rendant impossible d'assurer la continuité des activités critiques de l'organisation et de répondre aux objectifs de continuité.
Le chiffrage des solutions est tout aussi critique, car sans lui l'organisation ne peut pas prévoir et allouer le budget nécessaire au déploiement de celles-ci.

b) Evaluer la pertinence des solutions

Si l'organisation ne s'interroge pas sur la pertinence des solutions de continuité qu'elle envisage, les solutions qu'elle adoptera et mettra en place peuvent ne pas permettre de répondre aux objectifs de continuité, ne pas correspondre aux attentes de la Direction Générale ou entraîner des coûts supérieurs aux coûts d'une interruption d'activité. Il n'y a pas d'intérêt pour une organisation à déployer des ressources et moyens pour mettre en place un PCA totalement inadapté qui ne permet pas d'assurer la continuité de ses activités critiques.

c) Choix des solutions

Dans l'éventualité où la sélection des solutions retenues n'est pas officialisée, il est possible que les opérationnels responsables de la continuité de leur activité critique ne déploient pas la solution qui aurait dû être retenue pour cette activité mais une solution qui ne serait pas faisable, trop coûteuse ou non pertinente. Cela remet en cause à la fois l'efficacité du PCA, mais aussi son optimisation, et

gaspille également les ressources qui ont été mobilisées pour réaliser les études de faisabilité et de pertinence.

2.2.1.5 Etape 4 : Base documentaire

La non mise en place d'une base documentaire complète, efficace et pertinente pour l'ensemble des documents relatifs au PCA peut entraîner un certain nombre de conséquences dommageables pour l'organisation, telles que la perte, la destruction, la corruption ou le vol d'informations stratégiques et/ou confidentielles, ainsi qu'une difficulté accrue pour maintenir et mettre à jour le PCA.
En outre, dans le cas où le PCA de l'organisation est régi par des référentiels normatifs ou règlementaires, cela peut être préjudiciable dans le cadre d'audits externes ultérieurs, de conformité ou de certification, où l'organisation ne serait pas en mesure de produire les preuves de ses actions, ou encore si la traçabilité des documents elle-même est une obligation qu'elle ne respecterait alors pas.

2.2.1.6 Etape 5 : Politique de communication

a) Communication Interne

La communication interne revêt une importance de premier plan, puisque si celle-ci n'est pas convenablement planifiée et maîtrisée, le PCA de l'organisation peut être compromis.
En effet, si les collaborateurs ne sont pas informés en amont de la survenance d'un sinistre sur les dispositifs de continuité d'activité, ils ne sauront pas bien réagir dans l'urgence de la survenance d'un sinistre, et le déploiement du PCA ne sera pas optimal.
Pendant la crise, ces derniers ne sauraient être rassurés sans une bonne communication interne, et risqueraient alors de céder à un mouvement de panique où les procédures de continuité seraient difficilement appliquées et la crise peu maîtrisée. Cela peut rendre inopérant le PCA, prolonger la durée de la crise et en aggraver les conséquences, mais également, à terme, ternir l'image de l'organisation.
A l'issue de la crise, sans une officialisation du retour à la normale puis un débriefing et un retour d'expérience sur la crise, la transition sera plus longue et plus approximative, avec de probables erreurs en chemin. De plus, les collaborateurs n'auraient pas de retour sur les efforts exceptionnels qu'ils ont fourni, risquant de réduire leur motivation pour la survenance du prochain sinistre si ceux-ci ne sont pas valorisés. Enfin, les dispositifs de continuité ne peuvent pas faire l'objet d'une amélioration si on n'identifie pas et ne communique pas sur les pistes d'amélioration de ceux-ci.

b) Communication Externe

Dans le cas où la communication de l'organisation relative à son PCA vers l'externe serait insuffisamment planifiée et maîtrisée, il y aurait essentiellement des risques sur l'image de l'organisation, soit directement négatives de dégradation de celle-ci, soit de perte d'opportunité de l'améliorer et la promouvoir.
Ainsi, en amont de la survenance d'une crise, l'absence ou la mauvaise communication externe pourrait ne pas faire gagner, voire faire perdre à l'organisation des clients qui seraient sensibles aux problématiques de continuité d'activité mis en place par leurs fournisseurs. Cela pourrait également

inquiéter les investisseurs et partenaires s'ils ne sont pas convaincus de la résilience de l'organisation face à une éventuelle crise.
Pendant une crise, sans communication externe organisée, l'organisation est entièrement dépendante des médias et ne peut pas défendre et sauvegarder son image. Le public ne dispose que d'un seul son de cloche, ce qui n'est en outre pas très rassurant pour lui si l'organisation ne s'exprime pas.
A l'issue d'une crise, le public est avide d'explications et de retours d'expérience sur les évènements passés. Sans communication de la part de l'organisation, il restera sur sa faim, potentiellement mécontent, ou comblera ce vide par une autre communication sur laquelle l'organisation n'aura aucun contrôle et qui ne sera pas nécessairement une bonne chose pour son image.
D'une manière générale, que ce soit le silence total de l'organisation vis-à-vis de l'externe ou une communication incohérente et désorganisée, cela aura des conséquences néfastes sur son image.

c) Confidentialité

En l'absence de classification et de protection adaptée des informations sensibles liées au PCA, l'organisation prend le risque de perte, destruction, corruption ou vol de ces informations avec les conséquences en cascade que cela peut entraîner.

2.2.2 Risques liés au déploiement du PCA

2.2.2.1 Gestion de crise

a) Constitution d'une cellule de crise

L'absence ou la mauvaise constitution d'une cellule de crise présente le risque de ne pas avoir de responsables identifiés pour la veille des indicateurs d'activité, la remontée et la gestion des incidents, l'alerte et l'escalade, la gestion et la communication de crise, puis l'accompagnement de la sortie de crise et le retour à une situation normale avec un retour d'expérience sur la crise. Sans responsables identifiés, ces tâches seront moins bien organisées et moins bien réalisées, et l'organisation sera moins réactive et plus vulnérable aux impacts d'une crise.
Si la cellule de crise est mal constituée et ses membres mal identifiés, ou si ses fonctions, pouvoirs et responsabilités ne sont pas officialisés, celle-ci risque de ne pas disposer des compétences qui lui sont nécessaires pour mener à bien ses fonctions, et ne pas disposer de la légitimité et la confiance de ses interlocuteurs internes et externes.

b) Dispositifs de veille, de remontée et de gestion des incidents

En l'absence ou la non pertinence d'un dispositif de remontée et de gestion des incidents, le risque est que les incidents mineurs ne soient pas traités et se transforment systématiquement en crises de grande ampleur.
Dans le cas où le dispositif de veille est inexistant ou inopérant, l'organisation ne sera pas capable de détecter et d'anticiper la survenance d'un sinistre, et ne pourra donc pas préparer sa réaction. Elle sera donc plus vulnérable aux crises, avec un délai de réactivité plus long, subissant davantage d'impacts avant d'enclencher ses dispositifs de continuité d'activité.

c) Dispositifs d'alerte et d'escalade

A l'instar des dispositifs de veille, les dispositifs d'alerte et d'escalade permettent à l'organisation de préparer graduellement sa réaction à la crise, jusqu'à ce qu'elle soit officiellement déclarée. Ainsi, sans ces dispositifs, sa réaction est moins rapide, moins préparée et moins organisée, et elle subit plus gravement les impacts des sinistres.

d) Gestion de la crise et de la communication

Lors de la survenance d'une crise, si une organisation n'en maîtrise pas la gestion, les opérationnels n'obtiendront aucun soutien dans le déploiement de leurs PCA métiers et se contenteront d'appliquer les procédures de continuité. La gestion des imprévus risque de ne pas être optimale et entraîner des conséquences préjudiciables pour l'entreprise, et aucune coordination globale n'est garantie, notamment en termes d'allocation des ressources disponibles, de sécurité et de logistique.
En outre, si un journal de bord de la crise n'est pas tenu, la traçabilité des évènements ne sera pas garantie et le retour d'expérience moins aisé.

La communication de crise est également un point de contrôle clé dont la maîtrise est essentielle. Si elle ne l'est pas, cela peut entraîner la panique et la désorganisation des collaborateurs en interne, ainsi que l'inquiétude des partenaires et la dégradation de l'image de l'organisation en externe.

e) Sortie de crise et retour à une situation normale

Sans un suivi de l'évolution de la situation afin de déclencher les PRA au moment opportun, puis l'accompagnement de la sortie de crise, la situation dégradée risque d'être plus longue, augmentant d'autant les dommages subis par l'organisation.
Par ailleurs, si un retour d'expérience n'est pas réalisé à l'issue de la crise, l'organisation perd une occasion d'améliorer son dispositif de continuité à l'aide des dysfonctionnements et axes d'améliorations qu'il aurait permis de dégager.

2.2.2.2 Logistique de crise

Dans l'éventualité où une organisation ne met pas en place de logistique de crise, incluant notamment un site de repli, du matériel de secours et les moyens de transport permettant de déplacer des activités critiques et le personnel depuis le site sinistré vers le site de repli, sa continuité d'activité risque d'être compromise. En effet, si le sinistre endommage les infrastructures et équipements critiques qui sont absolument nécessaire au maintien d'un niveau de service minimum, les équipes ne disposeront pas des moyens nécessaires au déploiement du PCA.
Lorsque l'organisation a prévu un site de repli opérationnel mais pas la logistique de transport permettant de déplacer l'activité jusqu'à lui, ces infrastructures et équipements ne sont pas disponibles et le PCA ne peut pas être déployé.

2.2.2.3 Protection et sécurité du personnel

Une organisation qui ne prévoit pas la protection et la sécurité du personnel en cas de survenance d'une crise s'expose à des dégâts humains, qui la priveraient de ressources humaines potentiellement critiques pour le déploiement du PCA. Il faut également envisager le risque de sanction si l'organisation est reconnue responsable de ces dégâts humains, ainsi qu'un risque de dégradation de son image.

2.2.2.4 Implication des partenaires indispensables

Les partenaires indispensables sont essentiellement les partenaires de secours, dont les prestations doivent précisément se déclencher lors de la survenance d'une crise. S'ils ne sont pas impliqués et que le PCA de l'organisation reposait au moins pour partie sur la fourniture de ces prestations, elle peut ne pas disposer des ressources et moyens nécessaires au déploiement de son PCA.

2.2.2.5 Information et formation des acteurs impliqués

Sans une formation adéquate et de qualité dispensée aux acteurs du PCA, ceux-ci peuvent ne pas connaître leur rôle en situation de crise, avoir une réactivité plus lente et commettre des erreurs qui seraient préjudiciables à l'organisation, ou tout du moins augmenter sa vulnérabilité aux sinistres.
En outre, privé de formations, le personnel concerné perdrait l'opportunité d'un moment d'échange où il peut poser des questions et asseoir sa compréhension et son implication dans la démarche.

2.2.2.6 Implication et support de la Direction Générale

Une démarche de continuité d'activité qui ne bénéficie pas de l'implication et du support de la Direction Générale de l'organisation se retrouve privée d'une partie de sa légitimité, avec le risque d'une adhésion et d'une implication moindre de la part des collaborateurs. C'est par ailleurs la Direction Générale qui a le dernier mot sur l'allocation des budgets et ressources, et si son implication dans la démarche n'est pas totale, ces allocations au PCA risquent d'être limitées.

2.2.2.7 Mallettes de crise

L'absence de mallettes de crises dans une organisation prive les responsables de PCA métiers d'un outil précieux en situation de crise, avec le risque de la non optimisation de leur réactivité et du déploiement des solutions de continuité.

2.2.2.8 Premier test technique du PCA et validation

Si une organisation ne réalise pas un premier test technique du PCA avant sa validation, elle prend le risque que celui-ci, bien qu'il soit théoriquement opérationnel, soit en réalité défaillant. Elle constaterait alors cette défaillance dans une situation réelle de crise où les conséquences seraient bien plus grave que dans le cadre d'une simulation. Les acteurs du PCA n'auraient par ailleurs vécu aucun essai et seraient moins à l'aise dans leur rôle lors de la survenance d'une crise réelle.
Si un test ne porte pas sur toutes les composantes du PCA, le risque est que une ou plusieurs de ces composantes soient défaillantes et que cela ne soit pas détecté en amont de la survenance d'un sinistre.

Enfin, si l'organisation ne formalise pas un débriefing et un retour d'expérience sur ce test, elle se prive d'une opportunité de perfectionner son dispositif de continuité et de corriger les éventuels dysfonctionnements révélés par le test. Le personnel mobilisé pour le test n'est pas non plus valorisé pour les efforts qu'il a fournis dans le cadre du test, et il peut percevoir cela comme de l'ingratitude de la part de la hiérarchie, ce qui peut entacher sa motivation et son implication dans le PCA.

2.2.3 Risques liés à la maintenance du PCA

2.2.3.1 Veille des évolutions contextuelles

a) Facteurs d'évolution

Si une organisation ne réalise pas une veille active des différents facteurs dévolution du PCA que sont les règlementations et normes, la stratégie de l'organisation, le marché, les partenaires externes et le changement de personnel, elle peut ne pas avoir connaissance des évolutions majeures qui nécessitent une mise à jour de son dispositif de continuité d'activité. Sans ces informations, elle ne peut pas mettre à jour son PCA, qui risque alors de se retrouver inopérant, avec des acteurs non informés et formés, inadapté aux besoins de l'organisation ou non conforme aux règlementations, normes et exigences de la Direction Générale et des parties prenantes.

b) Mise à jour des cartographies des processus et des risques, des analyses d'impact et de la stratégie de continuité

Sans mise à jour régulière des cartographies des processus et des risques, des analyses d'impact et de la stratégie de continuité qui devraient être la suite logique des diverses évolutions contextuelles et stratégiques, le dispositif de continuité d'activité risque de ne pas être maintenu en condition opérationnelle. Il risque alors d'être inopérant et non conforme.

2.2.3.2 Tests réguliers du PCA

En l'absence de tests réguliers de son PCA, l'organisation n'est pas en mesure de s'assurer de l'absence de défaillances sur tout ou partie de celui-ci suite aux évolutions intervenues depuis son déploiement initial. De plus, le nouveau personnel impliqué ne bénéficie pas d'un exercice pratique pour se familiariser avec son rôle et ses responsabilités en cas de sinistre.
Sans retour d'expérience sur ces tests, le dispositif ne fait pas l'objet d'une amélioration continue et n'est donc pas optimal.

2.2.3.3 Mise à jour des évaluations financières

Si les évaluations financières du PCA ne sont pas mises à jour régulièrement, elles risquent d'être déconnectées de la réalité, et le budget et les ressources allouées en conséquence seront inadaptés, avec le risque qu'ils ne permettent pas le déploiement du dispositif en cas de besoin.

2.2.3.4 Mise à jour des procédures

Dans l'éventualité où une organisation ne mettrait pas à jour les procédures de son PCA, celles-ci risquent de devenir obsolètes et inopérantes le jour où elles seront déployées, ne permettant pas d'assurer la continuité des activités critiques de l'organisation à leur niveau de service minimum.

2.3 Risques spécifiques sectoriels

2.3.1 Secteur bancaire

Le secteur bancaire étant un secteur particulièrement critique et soumis à une règlementation dense, les risques qui lui sont spécifiques sont nombreux et très clairement identifiés :

- **Risque de contrepartie** : Lié à l'emprunteur qui pourrait faire défaut à ses obligations
- **Risque de liquidité** : Lié à la situation des banques et leur capacité à disposer des liquidités suffisantes pour faire face à leurs contraintes immédiates
- **Risque de taux** : Lié à l'évolution des taux d'intérêts fixés par les banques centrales et qui peuvent s'avérer défavorables pour les activités bancaires
- **Risque de change** : Lié à la variation défavorable des cours de devises
- **Risque de marché** : Lié à une variation défavorable des cours d'actifs financiers détenus par les banques
- **Risque pays** : Lié à un pays en particulier et à sa situation globale, qui peut être un problème si la banque y a des intérêts
- **Risque opérationnel** : Lié à la présence grandissante d'infrastructures techniques (systèmes d'information en particulier)
- **Risque de solvabilité** : Lié au fait que la banque ne dispose pas des fonds propres suffisants pour absorber ses pertes

C'est la vocation des instances de tutelle que de tenter de maîtriser ces risques pour réguler la stabilité des marchés financiers, et celle des banques que de se soumettre aux impératifs règlementaires pour limiter les impacts des différentes crises qu'elles traversent.

2.3.1.1 Risques majeurs d'indisponibilité de l'environnement de travail

Les risques majeurs d'indisponibilité de l'environnement de travail spécifiques au secteur bancaire sont identiques aux risques majeurs "causes" génériques, à savoir les sinistres naturels, technologiques, sociaux, économiques et politiques, sanitaires ou nucléaires, radiologiques, biologiques et chimiques, et aux risques "conséquences" qu'ils peuvent entraîner.
Les banques ont cependant l'obligation d'assurer la continuité de leurs activités et la grande majorité d'entre elles prévoit donc des sites de repli dans le cas où le site de travail principal ne pourrait pas être accessible.

2.3.1.2 Risques d'impacts liés aux points de contrôle clés de continuité

a) <u>Organisation et pilotage</u>

L'organisation et le pilotage de la démarche de continuité d'activité constitue un point de contrôle clé de la continuité d'activité, et l'absence de dispositifs de ce type conduirait à un risque de dispositif de continuité d'activité désorganisé et inefficace, ne permettant pas d'assurer la continuité des activités critiques de l'établissement.

b) Contrôles permanents et conformité règlementaire

Dans l'éventualité où les contrôles permanents et l'assurance de la conformité règlementaire ne seraient pas étendus aux dispositifs de continuité d'activité, l'organisation s'expose à la non couverture des risques critiques, concernés par la démarche PCA. La non-conformité potentielle aux dispositions règlementaires relatives aux PCA pourrait également entraîner des sanctions (notamment financières) de la part des instances de tutelle.

c) Plan de Sauvegarde Informatique (PSI)

Le principal risque associé à la mise en place d'un PCA dans un établissement bancaire est le risque qui pèse sur les SI. Outre les risques associés à la non disponibilité de l'environnement de travail, la continuité d'activité d'une banque repose principalement sur la viabilité des applicatifs critiques et l'accès aux bases de données essentielles. Dans l'éventualité peu probable où une banque en serait privée, son activité s'en trouverait paralysée, la continuité d'activité ne pourrait être assurée, et l'établissement subirait des dommages irréparables en quelques heures seulement.

d) Plan de repli utilisateurs

La mise en place d'un plan de repli utilisateurs constitue également une condition essentielle à la viabilité du dispositif de continuité d'activité. En effet, en l'absence de ce plan, l'établissement serait dans l'incapacité de déployer ses dispositifs de continuité, en l'absence ou l'indisponibilité du matériel et des moyens nécessaires (notamment informatiques). La continuité d'activité ne serait donc pas assurée.

e) PSEE

Il est nécessaire d'étendre la démarche de continuité d'activité aux prestataires de services essentiels externalisés, puisque cela constitue une obligation légale à laquelle sont soumis les établissements bancaires. Sans cela, ils s'exposent à une non-conformité et donc à des sanctions de la part des instances de tutelle.

2.3.2 Secteur de la santé publique

2.3.2.1 Risques majeurs d'indisponibilité de l'environnement de travail

Dans le cadre de la continuité d'activité, les établissements de santé doivent faire face à deux types de risques : Les sinistres internes à l'établissement, et les crises externes générant un afflux massif de victimes.

a) Le risque externe d'afflux massif de victimes

Les risques "causes" répondent à la même typologie que les risques majeurs génériques, à savoir les sinistres naturels, les sinistres technologiques, les sinistres sociaux, économiques et politiques, les sinistres sanitaires et les sinistres nucléaires, radiologiques, biologiques et chimiques.

Ces différents sinistres peuvent provoquer le risque "conséquence" spécifique d'un afflux massif de victimes auquel l'établissement de santé devra être en mesure de faire face.

b) Les risques internes à l'établissement de santé

En interne à un établissement de santé, les mêmes risques "causes" de survenance d'un sinistre majeur vont avoir des risques "conséquences" spécifiques, à la fois que l'organisation elle-même et sur ses partenaires, auxquels sera particulièrement sensible un établissement de santé. Les principaux risques "conséquences" se déclinent en quatre types :

- Les risques de défaillance du matériel biomédical
- Les risques techniques (perte d'alimentation en électricité, fluides, eau courante, oxygène, défaillance de la blanchisserie, des services d'hygiène, du service de restauration…)
- Les risques liés au Système d'Informations et Télécoms (perte de données, inaccessibilité aux applications, au dossier patient, défaillance des télécommunications, saturation des réseaux…)
- Les risques liés aux approvisionnements (ruptures de stocks de consommables, médicaments, sang…)

2.3.2.2 Risques d'impacts liés aux points de contrôle clés de continuité

a) Fonctionnement du matériel biomédical

Une interruption de fonctionnement du matériel biomédical peut conduire au report d'interventions, de rendez-vous… Un problème grave peut être préjudiciable pour le patient si la panne survient en cours d'intervention.

b) Services techniques

Une interruption de l'alimentation en énergie ou en fluides peut avoir des conséquences graves pour un établissement de santé, en provoquant une interruption de fonctionnement du matériel et des infrastructures, et donc en provoquant les conséquences de leur interruption.

c) Approvisionnements clés

Une interruption des approvisionnements clés d'un établissement de santé peut résulter en un report d'interventions, ou avoir des conséquences préjudiciables pour les patients en cas d'un besoin urgent.

d) Plan blanc interne et dispositif d'intégration dans les dispositifs globaux

L'absence de prévision de dispositifs de plan blanc interne et/ou d'intégration dans les dispositifs globaux peut résulter en des sanctions pour l'établissement de santé, puisqu'il s'agit d'une obligation règlementaire. Par ailleurs, l'établissement serait dans l'incapacité de réagir efficacement à une crise et plus vulnérable aux sinistres, incapable de gérer un afflux de victimes. Un risque d'image important pour l'établissement, ainsi que des potentiels dégâts humains sont à prendre en compte.

e) SIH (Système d'Information Hospitalier)

Dans le cadre d'un établissement de santé, des risques spécifiques sont associés au système d'informations. En effet, certaines données sont soumises au secret médical, et leur accès doit être sécurisé, afin d'éviter toute poursuite judiciaire de l'établissement. Par ailleurs, il est essentiel que le dossier patient soit toujours disponible, afin d'éviter des éventuelles erreurs médicales pouvant être préjudiciables pour les patients. Certaines applications critiques et le réseau doivent en outre disposer d'une continuité de fonctionnement afin d'éviter tout report d'intervention.

2.3.3 Secteur alimentaire

2.3.3.1 Risques majeurs d'indisponibilité de l'environnement de travail

La norme 22000 recense un certain nombre de risques "causes" spécifiquement liés à l'activité agroalimentaire :

- Incendie des bâtiments
- Inondations des zones de stockage
- Bioterrorisme ou sabotage
- Conditions climatiques extrêmes (canicule)
- Pannes énergétiques
- Accidents routiers
- Contamination soudaine de l'environnement immédiat
- Apparition d'un nouveau danger à prendre en compte, gestion de crise (TIAC)
- Panne d'un équipement contribuant à la sécurité des aliments (un détecteur de métal par exemple)

Une partie des risques et de la sinistralité dans l'agroalimentaire repose sur les catastrophes naturelles. Les installations sont souvent très imposantes et excentrées, donc plus exposées.
Mais au-delà des risques d'inondations et des risques naturels qui peuvent concerner les sites se situant dans d'autres régions du monde (pour les structures complexes), les deux grandes typologies de risques observées sont celles des risques d'incendie et des risques de contamination.

a) L'incendie

Les risques d'incendie représentent 40% des risques dans l'agroalimentaire.
Si les origines sont souvent les mêmes (défaut électriques, travail par point chaud, facteur humain etc.), il existe des facteurs inhérents à l'activité à l'origine de ces incendies :

- Le recours aux panneaux sandwich combustibles
- La présence de charges combustibles
- L'utilisation d'équipements spécifiques (friteuses à huile, fours industriels, brûleurs à gaz)

b) La contamination

Ce risque est sans doute le plus spécifique à l'agroalimentaire et le plus dangereux puisqu'il s'agit ici de santé publique. La contamination alimentaire peut en effet intervenir dans plusieurs cas de figure :

- Au cours d'un dégagement de fumée lors d'un incendie
- Lors d'une fuite d'un système de réfrigération à l'ammoniac à l'intérieur d'une chambre froide ou d'une salle de refroidissement

c) Protection de la production

A tous ces scénarios connus qui peuvent s'avérer désastreux pour la continuité d'activité, il faut opposer un système efficace de Contrôle Interne en accord avec la règlementation en vigueur.
Il faut également penser la continuité de façon globale en réfléchissant à une plus grande échelle. En effet, lors de la survenance de ces sinistres, il faut également réfléchir à l'interdépendance qui caractérise les unités de production dans l'agroalimentaire, et prévoir une solution de secours efficace dans le cas où l'une d'entre elle serait sinistrée. Les contraintes de livraison imposées par la grande distribution peuvent rapidement mettre à mal la situation financière des entreprises si elles n'ont rien prévu à ce niveau.

2.3.3.2 Risques d'impacts liés aux points de contrôle clés de continuité

a) Sécurité des infrastructures et sites de production

La continuité de la production repose sur la viabilité des sites de production. En cela, une indisponibilité des infrastructures et l'absence d'un site de repli seraient dramatiques en cas de sinistre. Cela paralyserait la production dans un secteur d'activité où la grande distribution ne transige pas sur les délais de livraison. La position de force des clients de l'agroalimentaire oblige les entreprises du secteur à se soumettre à leurs exigences au risque de perdre leurs marchés.

b) Equipements lourds de production

Les équipements lourds de production dans l'industrie alimentaire peuvent être source de problèmes très graves pour la continuité d'activité. Ils sont souvent la cause d'incendies dans les sites de production ou de rupture de la chaine du froid par exemple.

c) Chaine de production

La continuité de l'activité dans l'industrie agro-alimentaire repose aussi essentiellement sur la chaine de production, qui ne doit pas être interrompue. En effet il est rare qu'un même groupe s'occupe de toutes les étapes de la production des denrées alimentaires. Certaines d'entre-elles sont sous-traitées ou confiées à des partenaires. Il est tout aussi exceptionnel que toutes les étapes de production aient lieu au même endroit. Des relations d'interdépendance existent donc entre les différents acteurs de la production. Il est par conséquent capital que la coordination entre eux soit parfaite, notamment au niveau de leurs PCA, sous-peine de mettre en péril la continuité des activités.

d) Sécurité alimentaire

Il s'agit du volet le plus critique de l'activité. Au-delà des impacts en termes d'image qu'une crise sanitaire aurait sur un groupe industriel, les conséquences financières seraient désastreuses. En effet les règlementations imposent, lorsqu'il y a un doute sur un échantillon de denrées, de les retirer immédiatement de la commercialisation. Il y a également le cas des crises extrêmes comme celle de la vache folle, qui ont des conséquences dramatiques sur la santé de certains consommateurs.

e) Alimentation en énergie

De la même manière, l'industrie agroalimentaire a également besoin d'une continuité d'alimentation en énergie et de fonctionnement des infrastructures sur lesquelles elle repose.

2.3.4 Secteur de l'énergie

2.3.4.1 Risques majeurs d'indisponibilité de l'environnement de travail

Les risques majeurs d'indisponibilité de l'environnement de travail spécifiques au secteur énergétique répondent à la même typologie que les risques majeurs génériques, à savoir les sinistres naturels, technologiques, sociaux, économiques et politiques, sanitaires ou nucléaires, radiologiques, biologiques et chimiques, qui en sont les grands risques "causes", et aux impacts qu'ils peuvent entraîner.
Les organisations appartenant à ce secteur d'activité ont cependant une faible sensibilité à des risques "conséquences" spécifiques, que sont la destruction ou l'endommagement des infrastructures accueillant les fonctions supports, les risques critiques étant plutôt concentrés sur les installations de distribution et leur accessibilité par le personnel de terrain.

2.3.4.2 Risques d'impacts liés aux points de contrôle clés de continuité

a) Sécurité du réseau de distribution et de transport du gaz, ainsi que des installations

La continuité de la sécurisation du réseau de distribution et de transport, ainsi que de la viabilité des installations et infrastructures est essentielle dans cette activité. Le Ministère de l'Environnement et du Développement Durable précise que plus de 90% des explosions interviennent à cause de l'insalubrité des installations ou de leur vétusté. Il est indispensable de prendre des précautions quant à l'accès à ces installations qui ne sauraient être approchées que par des professionnels, au risque de s'exposer à des accidents très graves, possiblement lourds de pertes humaines.

b) Approvisionnement en gaz

La France n'est pas un producteur de gaz naturel. L'essentiel est importé de pays partenaires. Notre consommation dépend donc entièrement de la continuité de l'approvisionnement de nos fournisseurs en gaz, notamment la Russie. Il est par conséquent compréhensible que si ceux-ci venaient à arrêter l'approvisionnement, nous serions dans une situation dramatique de pénurie.

c) Espaces de stockage du gaz

Les espaces de stockage sont un élément de continuité à court terme, en réponse au risque de pénurie consécutive à l'arrêt potentiel des approvisionnements en gaz. Cependant, le stockage massif de gaz ou de gaz liquéfié présente des dangers non négligeables si les sites ne sont pas extrêmement sécurisés et surveillés.

d) Sécurité du personnel et des consommateurs

Un des impératifs spécifiques à l'activité de distribution du gaz est la sécurité du personnel et des consommateurs. En effet, l'acheminement du gaz présente des risques, au même titre que la maintenance des infrastructures ou encore l'intervention à la suite d'une alerte d'un consommateur. Des précautions sont à prendre pour éviter les accidents.

e) Ressources humaines

De la même manière, l'intervention sur les réseaux visant à résoudre les problèmes requiert de s'assurer de la compétence du personnel expert, au risque d'exposer les consommateurs comme le personnel à des accidents.

f) SI industriels

Enfin, la fiabilité des SI industriels est très importante pour la continuité d'activité, car ils sont le vecteur des « alertes réseaux » que sont le repérage des fuites, les systèmes de mesure à distance des niveaux, les systèmes d'alarme anti-intrusion… Sans les SI industriels, les opérateurs ne disposent plus de visibilité sur le réseau.

2.3.5 Secteur des transports

2.3.5.1 Risques majeurs d'indisponibilité de l'environnement de travail

Les risques "causes" auxquels sont vulnérables les organisations appartenant au secteur des transports relèvent de la même typologie que les risques génériques communs à toutes les organisations, c'est la sensibilité aux impacts qui va être spécifique.

Ainsi, certains aléas météorologiques (orages, neige…), climatiques (inondations, incendies…) et catastrophes naturelles ont des risques "conséquences" importants sur les organisations de transport, notamment en termes d'endommagement ou de destruction des infrastructures, un accroissement du risque d'accidents, ayant pour conséquences des risques de panne ou défaillance des infrastructures, du matériel ou des SI, d'interruption de l'alimentation en énergie, fluides ou télécommunications, de troubles de la sûreté et de la sécurité des personnes, une restriction des capacités et une perte de qualité de service.
Ces évènements peuvent par ailleurs impacter les partenaires externes de l'organisation, avec un risque de rupture des approvisionnements et donc de rupture de stocks critiques, pouvant paralyser l'activité.

Les sinistres de type industriels, comme par exemple des accidents (collisions, déraillements de trains, crashs d'aéronefs, explosion de sites…) ou des fuites de carburants ou autres produits

dangereux, que la responsabilité de l'organisation soit engagée ou non, ont des risques "conséquences" similaires à ceux des catastrophes naturelles, avec l'ajout d'un important risque d'image du à l'écho médiatique.
C'est également le cas dans le cadre des actes de terrorismes et des évènements géopolitiques, troublant l'ordre public et pouvant également entraîner une dégradation du climat social, un éventuel mouvement de grève venant réduire voire interrompre l'activité.
Les risques liés aux erreurs et à la malveillance humaine sont également à considérer dans le cadre des transports.

Enfin, de par leur fonction de service public, les organisations relevant du secteur des transports doivent intégrer dans leur démarche de continuité d'activité des éléments de risques complètement indépendants de leur fonctionnement mais pour lesquels une réaction de leur part est attendue. Dans le cas de l'aviation civile, cela se manifestera par exemple par un aéronef en détresse nécessitant un atterrissage d'urgence que l'aéroport devra être en capacité d'accueillir.

2.3.5.2 Risques d'impacts liés aux points de contrôle clés de continuité

Dans l'éventualité où les dispositifs visant à assurer la continuité et la reprise des activités critiques de l'organisation sont inexistants ou inefficaces, l'organisation s'expose à des risques importants.

a) Sûreté et sécurité des personnes

En ce qui concerne la sûreté et la sécurité des personnes, une non garantie de celle-ci peut résulter en d'importants dégâts humains, et donc à des conséquences juridiques, financières (amendes, indemnisations et dédommagements), et d'image. Si la sécurité du personnel n'est pas assurée, l'indisponibilité de celui-ci nuira à la reprise des activités.

b) Continuité des services techniques

Une absence ou une mauvaise continuité des services techniques, et notamment de l'alimentation en énergie et fluides est un scénario d'empêchement impactant la continuité des autres activités critiques et provoquant donc leurs impacts.

c) Continuité de l'information aux voyageurs

La continuité de l'information aux voyageurs est une exigence règlementaire, et sa non-garantie pourrait résulter en des sanctions juridiques, sans compter l'insatisfaction des voyageurs et donc des risques d'image.

d) Viabilité hivernale

En ce qui concerne la viabilité hivernale, des engagements ont été pris par bon nombre d'organisations autour de la continuité d'activité en saison hivernale, et le non-respect de ceux-ci pourrait entraîner des sanctions. Par ailleurs, cela entraînerait inévitablement une baisse de l'activité et donc des pertes financières. L'image de l'organisation pourrait en outre être affectée.

e) Gestion de crise

Les dispositifs de gestion de crise sont un facteur clé de succès du déploiement des dispositifs de continuité. Sans elle, même les dispositifs les mieux conçus seront inopérants. En effet, elle se charge de la détection des incidents et pilote la réaction de l'organisation. En ce qui concerne la notification des incidents et du retour d'expérience, il s'agit d'obligations règlementaires, dont le manquement pourrait impliquer des sanctions.

f) Spécificités de l'aviation civile

Les spécificités de l'aviation civile que sont le péril animalier et l'aide à la navigation nécessitent des dispositifs de continuité d'activité afin d'éviter les accidents d'aéronefs contre lesquels ces activités critiques assurent une protection. En effet, en l'absence de guidance des appareils, le risque d'accident est important, de même qu'un oiseau qui serait piégé dans un réacteur d'avion pourrait faire exploser celui-ci. Il n'est nul besoin de préciser les impacts d'un accident d'aéronef, tant en terme humain, matériel et financier que d'image.

2.3.6 Secteur des télécommunications

2.3.6.1 Risques majeurs d'indisponibilité de l'environnement de travail

Les risques majeurs d'indisponibilité de l'environnement de travail, risques "causes", spécifiques au secteur des télécommunications répondent à la même typologie que les risques majeurs génériques, à savoir les sinistres naturels, technologiques, sociaux, économiques et politiques, sanitaires ou nucléaires biologiques et chimiques, et aux conséquences qu'ils peuvent entraîner.
Les organisations appartenant à ce secteur d'activité ont cependant une sensibilité accrue à des risques "conséquences" spécifiques, que sont la destruction ou l'endommagement des infrastructures et du matériel, l'interruption de l'alimentation en énergie, une indisponibilité de tout ou partie de leur personnel, ou encore l'interruption des approvisionnements clés tels que les puces électroniques, dans le cas où un sinistre affecterait leurs prestataires et fournisseurs. Un risque d'endommagement du système d'informations est également un point de vulnérabilité important.

2.3.6.2 Risques d'impacts liés aux points de contrôle clés de continuité

a) Système d'information

La continuité de fonctionnement et d'accessibilité du réseau des télécommunications repose en grande partie sur la stabilité du système d'informations de l'organisation qui l'administre. Une défaillance de la continuité de ce système d'informations pourrait causer une panne du réseau.
A travers les organisations du secteur des télécommunications circule une quantité importante d'informations, dont certaines sont confidentielles. Si la sécurité de celles-ci n'est pas garantie, l'organisation encourt des poursuites juridiques de la part de ses clients dont les données n'étaient pas protégées. Il peut également y avoir des conséquences en cascade liées à la fuite de certaines informations sensibles.

b) Infrastructures et alimentation en énergie

De la même manière que la stabilité du réseau repose sur la continuité du système d'informations, celle-ci nécessite une continuité d'alimentation en énergie et de fonctionnement des infrastructures sur lesquelles il repose.

c) Approvisionnements Clés

Certains approvisionnements sont essentiels pour le quotidien des opérations, et une rupture de stock sur ces éléments pourrait conduire à une interruption de fonctionnement du réseau. Ce serait notamment le cas dans l'éventualité d'une panne de matériel pour laquelle l'organisation ne disposerait pas des pièces de rechanges et fournitures nécessaires à sa réparation.

d) Ressources Humaines

Le personnel d'une organisation appartenant au secteur des télécommunications est également essentiel à son activité, et une insuffisance des effectifs peut perturber son efficacité et son efficience, voire provoquer une indisponibilité du réseau.

Une panne ou une indisponibilité du réseau, même temporaire et très courte, constitue une défaillance de l'opérateur au regard de ses obligations de service public, et au-delà des potentielles sanctions que celui-ci encourt, cela pourrait avoir des conséquences graves pour les utilisateurs de ce réseau.

2.4 Quelques exemples de sinistres célèbres

La sensibilisation des organisations aux grands risques qui les menacent découle beaucoup du constat de l'occurrence de sinistres graves, de la réalité du risque. Il s'agit d'une prise de conscience par la peur d'expériences qu'elles ont vécues ou dont elles ont été témoin.
Historiquement, beaucoup des impacts des différents sinistres auraient pu être minimisés par un bon dispositif de continuité d'activité. Nous avons cherché à lister ci-après quelques exemples de ces sinistres.

2.4.1 Catastrophes naturelles

- Cyclones en Polynésie Française en 1903 et 1983
  (Les conséquences furent bien moindres lors du 2ème cyclone, la résilience avait été accrue par un retour d'expérience suite au 1er sinistre)
- Tempête de Décembre 1999
- Canicule en 2003
- Tsunami dans l'Océan Indien en 2004
- Ouragan Katrina aux USA en 2005
- Tremblement de terre et tsunami au Japon en 2011

2.4.2 Sinistres technologiques

- Explosion d'AZF en 2001
- Catastrophe du tunnel sous le Mont Blanc en 1999
  (Condamnation pour non-réalisation d'exercices)
- Coupures massives d'électricité en Amérique du Nord en 2003
- Panne de BlackBerry en 2011
  (Associée à une mauvaise politique de communication, l'entreprise a été sérieusement mise à mal)
- Panne de l'opérateur téléphonique Orange en 2012

2.4.3 Sinistres sociaux, économiques, politiques

- Attentat de New-York en 2001
- Attentats de Londres en 2005
- Emeutes de la faim en 2008
- Printemps Arabe en 2011

2.4.4 Crises sanitaires

- Epidémie de Choléra à Londres en 1854
- Scandale de l'amiante dans les années 1970, puis les années 1990
- Affaire de la vache folle en 1996
- Affaire du sang contaminé en 1999
- Epidémie de SRAS à Hong Kong en 2003

- Grippe aviaire – Virus H5N1 en 2006
- Pandémie grippale - Virus H1N1 en 2009

2.4.5 Sinistres nucléaires, radiologiques, biologiques ou chimiques

- La catastrophe de Tchernobyl en 1986

2.4.6 Zoom sur un retour d'expérience de Benchmark : Accident nucléaire de Fukushima (11/03/2011, Japon)

2.4.6.1 Contexte et causes du sinistre

Ce sinistre a initialement touché la centrale nucléaire japonaise de Fukushima Daiichi.
Le séisme du 11 mars 2011 a entraîné un arrêt automatique des réacteurs de la centrale, la perte accidentelle de l'alimentation électrique et le déclenchement des groupes électrogènes.
À la suite du tsunami, des groupes électrogènes de secours sont tombés en panne. Des débris ont pu obstruer des prises d'eau. Ces défaillances, couplées à plusieurs erreurs humaines, ont causé l'arrêt des systèmes de refroidissement de secours des réacteurs nucléaires. Le défaut de refroidissement des réacteurs a induit des fusions partielles des cœurs de trois réacteurs nucléaires puis d'importants rejets radioactifs.
Des incendies suivis d'explosions vont contribuer à ruiner définitivement les installations et relâcher des quantités massives d'effluents radioactifs gazeux qui seront suivies par d'importantes masses d'effluents radioactifs liquides à la suite des lâchers d'eau entrepris par l'exploitant pour tenter de refroidir l'installation.
Cet accident nucléaire majeur est classé au niveau 7 (le plus élevé) de l'échelle internationale des événements nucléaires, ce qui le place au même degré de gravité que la catastrophe de Tchernobyl, en 1986.
À la suite du tremblement de terre et du tsunami, la centrale nucléaire de Fukushima Daini (incident de niveau 3) et la centrale nucléaire d'Onagawa ont également été endommagées.

2.4.6.2 Conséquences et impacts du sinistre

De nombreuses villes et zones portuaires ont été partiellement détruites. Les pertes économiques estimées sont de l'ordre de 210 milliards de dollars. La reconstruction prendra plusieurs années et son coût estimé en fait déjà l'un des séismes les plus onéreux de l'Histoire.
D'après l'Organisation Mondiale de la Santé (OMS), les conséquences sanitaires anticipées des doses d'irradiations reçues par les populations au Japon et en dehors sont minimes : Les niveaux d'incidence prédits par les modèles sont faibles, et aucune augmentation observable du taux de cancer n'est attendue.
Des mesures d'interdiction sur la commercialisation de produits contaminés ont été prises, avec l'évacuation des zones à risques. Cela, couplé avec la défaillance du fournisseur d'énergie qu'était la centrale nucléaire de Fukushima, a fortement impacté les acteurs économiques locaux.

2.4.6.3 Analyse des dispositifs de continuité

Le séisme n'est responsable que de peu de victimes et dégâts grâce à la qualité des constructions parasismiques japonaises. L'ampleur de cette catastrophe résulte essentiellement du tsunami qui s'ensuivit. Le gouvernement japonais a déclaré l' "état d'urgence nucléaire" pour le pays, et de nombreux habitants sont évacués, pour une situation finalement placée au niveau 7, le plus élevé, sur l'échelle internationale des événements nucléaires (INES) des accidents nucléaires et radiologiques. Les plans d'urgence gouvernementaux ont ainsi été efficacement déployés.
Dans le cas spécifique de la centrale nucléaire, l'installation avait été bâtie pour résister à un séisme de magnitude 8 et à un tsunami de 5,7 mètres de haut, or elle a subi un séisme de magnitude 9 (le plus important jamais enregistré au Japon) et un tsunami d'une hauteur de 15 mètres.
La centrale disposait de dispositifs de continuité en place et opérationnels. En effet, l'émission de gaz toxiques et la surchauffe ont été détectées, ce qui prouve qu'une certaine surveillance était réalisée. De plus, des groupes électrogènes ont pu pallier à la rupture d'alimentation électrique externe, et des systèmes de refroidissement de secours étaient prévus. Ces dispositifs se sont avérés insuffisants devant l'ampleur de la catastrophe et les imprévus liés.

2.4.6.4 Remarque : La continuité d'activité des partenaires comme point de contrôle clé du PCA

La catastrophe industrielle de Fukushima a perturbé l'ensemble de l'économie locale. Elle a notamment provoqué l'interruption de la production de Nissan (partenaire de Renault), privant Renault de ses approvisionnements clés ; Renault n'avait pas prévu de dispositif de continuité d'activité et a subi une interruption momentanée de sa production.
Ca cas particulier illustre très bien l'importance de l'intégration des partenaires et filiales dans la stratégie globale de continuité d'activité.

2.5 L'Articulation avec les autres dispositifs de maîtrise des risques

Les dispositifs mis en place dans le cadre de la continuité d'activité et la gestion de crise s'inscrivent dans la démarche de contrôle interne et plus généralement de maîtrise des risques d'une organisation. Ils vont donc s'articuler avec les autres structures de la démarche, que sont le Management des Risques, les assurances, le Contrôle Interne et l'Audit Interne.
Afin de garantir une coordination optimale des différentes structures entre elles, les bonnes pratiques préconisent la présence de représentants des autres fonctions liées à la maîtrise des risques dans les organes de gouvernance du PCA.

2.5.1 Articulation avec le Management des Risques

La cartographie des risques est une base de données précieuse pour la conception d'un PCA, qui sera utilisée dans le cadre de l'établissement de la cartographie des risques PCA, visant à identifier les risques majeurs d'indisponibilité de l'environnement de travail auxquels l'organisation est vulnérable et contre lesquels le PCA va permettre de se prémunir.

2.5.2 Articulation avec les assurances

La politique d'assurance de l'entreprise est un élément de maîtrise des risques, et doit donc être prise en compte dans la conception du PCA, afin de le concevoir en adéquation et en complément de celle-ci. L'objectif est à la fois de palier aux éventuelles défaillances assurantielles, mais également d'éviter les redondances de dispositifs, qui gaspilleraient les ressources de l'organisation.

2.5.3 Articulation avec les autres volets du Contrôle Interne

Il est essentiel de s'intéresser à l'ensemble des dispositifs de Contrôle Interne de l'organisation dans le cadre d'une démarche PCA. En effet, pour les risques majeurs d'indisponibilité de l'environnement de travail, il peut exister, préalablement au PCA, d'autres dispositifs de Contrôle Interne concourant à la maîtrise de ces risques. Il est nécessaire de recenser, d'analyser et de prendre en compte ces éléments pour garantir la pertinence du PCA. L'objectif sera de palier aux éventuelles défaillances identifiées, et d'éviter les redondances de dispositifs, qui gaspilleraient les ressources de l'organisation. En outre, l'implication d'un représentant de la gouvernance de l'ensemble du Contrôle Interne au sein des organes de gouvernance du PCA peut permettre de disposer d'une vision globale des sujets traités, notamment au niveau règlementaire et sur les différentes activités. Ce représentant peut avoir un œil averti sur la manière dont le responsable du projet veut le lancer et sur l'offre proposée par les éventuels prestataires de secours. Il peut également fournir un avis critique sur les dispositifs de maîtrise des risques et de continuité d'activité en place chez les partenaires fournissant des services en amont et en aval de l'organisation. La collaboration étroite avec les autres volets du Contrôle Interne permet d'assurer une coordination pertinente entre les l'ensemble des dispositifs de Contrôle Interne et le PCA. Il pourra également aider à définir les indicateurs de continuité d'activité, à la fois les indicateurs d'activités servant à la veille permanente pour la détection et l'anticipation des incidents, mais également les indicateurs du PCA lui-même, servant de base au reporting PCA. Associé au pilotage du projet, le Contrôle Interne fournit un gage de conformité du projet à la Direction Générale.

2.5.4 Articulation avec l'Audit Interne

Le PCA s'appuie sur l'Audit Interne, notamment dans le cadre de la maintenance de celui-ci, mais peut également le mobiliser plus en amont dans le projet. Il est important de veiller à sauvegarder l'indépendance et l'objectivité de l'Audit Interne lorsqu'il est mobilisé lors du projet PCA, et son implication doit se limiter à l'information. En effet, le rôle principal de l'Audit Interne dans la démarche de continuité d'activité consiste à auditer le PCA régulièrement, afin de l'optimiser, le mettre à jour et le maintenir en condition opérationnelle. Il est donc essentiel que l'Audit Interne n'ait pas été trop impliqué en amont pour que ces audits soient pertinents.
L'Audit Interne pourra cependant faire part de ses constats, notamment les faiblesses de Contrôle Interne identifiées lors d'audits précédents, et qui peuvent fournir une aide intéressante dans le cadre du projet PCA et de son analyse des dispositifs existants. Sa présence lors des séances des organes de gouvernance du PCA permet de cadrer en collaboration l'inscription du PCA au plan d'audit annuel et les modalités de ces audits.

2.5.5 Charte du PCA

De la même manière que l'on retrouve souvent dans les organisations des chartes du Contrôle Interne et de l'Audit Interne, la formalisation d'une charte du PCA peut être envisagée.
Cette charte présenterait la démarche PCA, avec ses grands principes et les enjeux, son rôle et ses objectifs. Prenant en compte la règlementation et les bonnes pratiques applicables, elle pourrait constituer un support de communication interne et de sensibilisation des collaborateurs intéressant.
Elle décrira les diverses modalités pratiques, mais aussi de gouvernance et de contrôle de la mise en place du PCA, et appuiera son maintien en condition opérationnelle, en imposant une fréquence de révision et de validation. Elle pose les obligations et l'environnement de contrôle nécessaire au bon fonctionnement du PCA, et confirme la nécessité de prendre en compte la continuité d'activité dans les nouveaux projets et développements.
Elle sert l'objectif de faire vivre la continuité d'activité initié lors du projet PCA et qui doit se maintenir dans la durée, mais également de faciliter le dialogue entre les acteurs du PCA. En s'intéressant à la pérennité des activités, elle prend sa place dans le système de maîtrise des risques et facilite l'insertion de la démarche de continuité d'activité dans la culture de l'organisation.
Cette charte se rapporte à l'ensemble des activités de l'organisation, et concerne toutes ses entités juridiques. Elle garantit la conformité des relations contractuelles entre l'organisation et ses partenaires externes concernés par la continuité d'activités. Elle garantit également la prise en compte de la continuité d'activité dans le Management des Risques.
Elle vise par ailleurs à légitimer les différents acteurs du PCA, notamment le RPCA, RPSI et les CCA, ainsi que les organes de gouvernance du PCA, en définissant précisément leurs rôles, pouvoirs et responsabilités.
Elle couvre l'ensemble des éléments qui constituent le PCA, en particulier les tests et exercices et la politique de communication, le reporting et la documentation du plan. Elle s'intéresse également à la sensibilisation, l'information et la formation du personnel, et à l'actualisation de celles-ci. Au niveau du budget, elle précisera les modalités d'engagement budgétaire en adéquation avec les efforts demandés par la continuité d'activité.

Synthèse de la seconde partie

- Les risques liés à la continuité d'activité d'une organisation, de la couverture desquels l'audit cherchera à s'assurer, peuvent être classifiés selon la typologie suivante :
  - Les risques d'indisponibilité de l'environnement de travail
    - Risques "causes"
    - Risques "conséquences"
  - Les risques liés aux points de contrôle clés de la démarche PCA
    - Scénarios d'empêchement
    - Impact des points de contrôle clés

<u>Les risques d'indisponibilité de l'environnement de travail</u>

- Le PCA d'une organisation visant à préserver celle-ci des impacts des risques majeurs auxquels elle est vulnérable, sinistres de grande ampleur aux conséquences dévastatrices, il est essentiel de bien les identifier. Ces grands sinistres constituent des risques "causes".
  Il s'agit essentiellement des catastrophes naturelles, des sinistres technologiques, des sinistres sociaux, économiques et politiques, des crises sanitaires, ainsi que des sinistres nucléaires, radiologiques, biologiques et chimiques.
- C'est cependant aux impacts potentiels de leur occurrence que les organisations sont réellement sensibles, et contre lesquels elles vont chercher à se prémunir à travers la mise en place d'un PCA. Ces impacts potentiels constituent les risques "conséquences".
  Ils diffèrent en fonction des risques "causes", mais regroupent globalement le risque de destruction ou d'endommagement des infrastructures et du matériel, d'indisponibilité du SI, de dégâts humains privant l'organisation de personnel, les risques juridiques et d'image, de pertes financières importantes ou de défaillance des fournisseurs de services essentiels (télécommunications…). Ces risques portent sur l'indisponibilité de l'environnement de travail d'une manière générale.
  En outre, et pour les secteurs d'activité critiques responsables d'un service public, cela peut nécessiter la fiabilité incontestable de leur continuité d'activité, voire une intervention renforcée dont dépendent d'autres organisations (télécommunications, santé publique…).
- La plupart des risques "causes" d'indisponibilité de l'environnement de travail sont communs à l'ensemble des secteurs d'activité, c'est la sensibilité à leurs différentes "conséquences" qui va réellement différencier les secteurs d'activités entre eux.

<u>Les risques liés aux points de contrôle clés de la démarche PCA</u>

- Les scénarios d'empêchement sont les éléments qui peuvent potentiellement entraver la correcte mise en place des points de contrôle clés du PCA. Ceux-ci sont détaillés ci-après et intégrés au guide d'audit des PCA.
- Les risques d'impact des points de contrôle clés concernent quant à eux les conséquences de l'incorrecte ou de la non mise en place des différents points de contrôle clés du PCA. De l'imperfection du dispositif et du gaspillage de ressources, ces impacts peuvent aller jusqu'à l'inefficacité ou la non-conformité règlementaire du PCA dans son ensemble, selon le point de contrôle considéré.

3. Guide d'audit des plans de continuité d'activité

Lorsqu'un projet PCA est mis en place dans une organisation, il s'agit d'un processus complètement nouveau, auquel l'Audit Interne doit prêter une attention particulière. La continuité d'activité n'est pas un sujet qui est nécessairement maîtrisé par l'Audit Interne, il ne dispose pas forcément de référentiels pour en guider l'audit et ne connait pas toujours la meilleure méthodologie et les meilleurs outils et techniques pour auditer un PCA. Ainsi, dans les premières années de vie du PCA, son inscription au plan d'audit sera minutieusement préparée, puis deviendra plus automatisée au fur et à mesure que les dispositifs deviennent opérants et entrent dans les mœurs.
Dans un premier temps, l'Audit Interne pourra envisager de s'appuyer sur le renfort d'une ressource externe pour auditer le PCA de l'organisation.

Dans le cadre de l'audit du PCA, L'Audit Interne va au-delà des exigences règlementaires, et rapproche les pratiques de l'organisation d'un référentiel de bonnes pratiques en la matière, pouvant s'appuyer sur les normes. Ce référentiel sera construit à l'aide des objectifs de l'organisation et de la stratégie de continuité, afin de pouvoir valider que les dispositifs de continuité d'activité y sont adaptés et que les budgets et efforts déployés sont en adéquation avec les enjeux.

L'Audit Interne peut être mobilisé en amont lors du projet PCA, au travers de sa connaissance des métiers de l'entreprise et des dispositifs de maîtrise des risques existants, et notamment de leurs défaillances. Dans le cas où l'Audit Interne prend part au projet PCA, il est essentiel de veiller à ce qu'il ne s'agisse que d'échange d'information et non d'une implication plus stratégique ou d'une validation par l'Audit Interne des décisions au fil de l'eau. L'Audit Interne doit en effet conserver son indépendance et son objectivité par rapport au PCA, afin que les audits qu'il mènera par la suite dans le cadre de son maintien en condition opérationnelle restent pertinents et apportent une véritable valeur ajoutée par la remise en question des dispositifs.

Le présent guide d'audit se base sur un découpage du processus de mise en place d'un PCA, identifiant les différentes étapes de la démarche, qui constituent les composantes du contrôle interne. A ces étapes sont associés des objectifs de contrôle interne et d'audit, avec les risques qui les menacent, à la fois génériques pour tout type d'organisation et spécifiques pour les secteurs d'activités critiques, ainsi que des points de contrôle clés visant à les couvrir. Il propose ensuite quelques bonnes pratiques de Contrôle Interne observées à travers des recherches et recueils de témoignages, vers lesquels les dispositifs devraient idéalement tendre, et les techniques d'audit permettant d'évaluer l'efficacité et l'efficience des contrôles mis en place. Il fournit les outils aux auditeurs internes pour les accompagner dans l'audit du PCA de l'organisation.

3.1 Objectif de l'Audit des PCA

L'audit des PCA peut servir deux objectifs majeurs. Il peut tout d'abord être utilisé comme préalable au projet PCA, afin de fournir un état des lieux de la situation, des dispositifs de maîtrise des risques en place et de leurs éventuelles défaillances. Il peut également permettre de valider l'opportunité de la mise en place d'un tel dispositif. Il s'agit de l'audit préalable à la mise en place d'un PCA.
Mais l'audit des PCA consiste aussi et surtout à s'assurer que le PCA répond à la stratégie de continuité et qu'il permet à l'organisation d'assurer la continuité et la reprise de ses activités critiques en cas de sinistre qui viendrait la priver de son environnement normal de travail.

Les objectifs de contrôle interne et d'audit par composante du contrôle interne sont détaillés dans le guide d'audit ci-après. Compte tenu des nombreux objectifs d'audit et du caractère évolutif du PCA, l'audit des PCA s'inscrit dans son maintien en condition opérationnelle, et il est recommandé de l'inscrire régulièrement au plan d'audit. Cela assurera une bonne mesure de l'efficience du processus et de la maîtrise des risques résiduels.

3.2 Méthodologie générale

A l'instar de toute mission d'audit, la mission d'audit des PCA doit être préalablement cadrée et ses modalités précisées. En effet, des dispositions du Cadre de Référence International des Pratiques Professionnelles (CRIPP) de l'Audit Interne rendent obligatoires :

- La conception et la formalisation du programme de travail de chaque mission. Ce programme précise le champ d'intervention, les objectifs, la date et la durée de la mission, ainsi que les ressources allouées (Norme Professionnelle 2200 "Planification de la mission")
- La délimitation du champ de la mission "qui doit être suffisant pour répondre aux objectifs de la mission" (Norme Professionnelle 2220 "Champ de la mission"). Le périmètre d'intervention doit notamment permettre d'apprécier le niveau d'exposition aux risques
- La détermination des ressources appropriées pour atteindre les objectifs de la mission. La Norme 2230 préconise notamment que "la composition de l'équipe doit s'appuyer sur l'évaluation de la nature et de la complexité de la mission, des contraintes de temps et des ressources disponibles".

L'audit des PCA est une mission de grande ampleur, qui comporte un volet assurantiel de conformité du dispositif au référentiel des bonnes pratiques et à la législation, et un volet de conseil concernant l'efficacité et l'efficience des choix opérés par rapport aux risques identifiés. Dans le cadre du conseil, il faut veiller à ce que l'indépendance et l'objectivité de l'Audit Interne ne soient pas compromises pour les missions futures. Cela peut se faire en formalisant en amont les attentes du commanditaire de l'audit, généralement la Direction Générale.

Le périmètre de la mission peut varier selon les cas. En effet, elle peut porter sur tout ou partie du PCA d'une organisation (PSI, PCA métiers, Gestion de crise…), et peut également être segmentée géographiquement par site ou juridiquement par entité de l'organisation (filiales).
La constitution de l'équipe d'audit doit être cohérente avec les enjeux de la mission, et doit regrouper les compétences spécifiques nécessaires (connaissance des métiers, finance et budget, systèmes d'information, gestion des ressources humaines…).

Le programme de travail de la mission, et notamment les objectifs d'audit, sont définis à partir de l'analyse des risques et du référentiel des bonnes pratiques de Contrôle Interne visant à leur maîtrise. Sont ensuite déclinés les techniques d'audit et outils permettant de répondre aux objectifs d'audit dans le guide d'audit ci-après.

Afin de mener sa mission à bien, l'Audit Interne devra avoir accès à l'ensemble de la documentation du PCA, et être en mesure de rencontrer les acteurs internes et externes de la démarche qu'il jugera pertinents. Parmi ces éléments, il recueillera notamment les rapports des anciens audits et études menés sur le sujet, afin de s'assurer du suivi de ces démarches.

Dans le cas d'un audit parcellaire sur une partie du PCA, sur un site ou une entité du groupe, il convient de prendre en compte les autres éléments et la manière dont ils s'articulent pour avoir une vision d'ensemble et une correcte identification des causes des dysfonctionnements éventuellement constatés.

3.3 Guide d'Audit des PCA : Référentiel Générique

3.3.1 La conception du PCA

Etapes de mise en place d'un PCA et d'une gestion de crise : Composantes du Contrôle Interne		Finalités : Objectifs de Contrôle Interne Objectifs d'Audit	RISQUES			Bonnes pratiques de Contrôle Interne	Techniques d'audit
			Facteurs (Scénarios d'empêchement)	Points de contrôle	Impacts		
Préalable : Communication Interne		S'assurer que la démarche PCA a fait l'objet de la diffusion d'un message S'assurer que tous les collaborateurs ont été destinataires du message S'assurer qu'ils l'ont compris S'assurer qu'il a été porté par la DG S'assurer de la qualité du message S'assurer qu'il en découle une implication des collaborateurs	Non-implication des collaborateurs Engagement de la Direction Insuffisant Message inadapté, incohérent, incomplet ou non clair	Mise en place d'une communication interne préalable à la démarche PCA	Non sensibilisation du personnel, mauvaise compréhension du concept, de l'intérêt et des enjeux Désintérêt et manque de motivation du personnel	Sensibilisation de l'organisation à la gestion des risques et à la continuité d'activité Préparation de la conduite du changement Engagement de la DG	Transmission et compréhension du message, implication : Sondage transverse du personnel (échantillon représentatif) Implication de la Direction Générale : Etude des supports de communication Qualité : Etude du message
Etape 1 : Constitution de l'équipe PCA		S'assurer de la bonne identification des acteurs S'assurer de la bonne définition des rôles, responsabilités, pouvoirs et délégations S'assurer de la bonne formalisation des éléments	Mauvaise identification des acteurs (fonctions incompatibles, compétences inadaptées, absence de crédibilité et légitimité) Mauvaise définition des rôles, responsabilités, pouvoirs et délégations Absence ou mauvaise formalisation des éléments	Désignation des acteurs PCA et formalisation de leurs rôles, responsabilités et pouvoirs	Equipe PCA inadaptée ou non compétente pour mener à bien le projet	Constitution d'organes de gouvernance du PCA (Comité de Pilotage et Comité Opérationnel), désignation d'un RPCA et d'un RPSI, ainsi que des CCA Définition des rôles, responsabilités et pouvoirs de ces différents acteurs	Etude du profil des acteurs (en particulier de leur fonction dans l'organisation) Revue des fiches de postes et lettres de missions Etude du schéma délégataire Vérification de la comitologie
Etape 2 : Définition des activités critiques et de la stratégie de continuité	Identification des activités critiques	S'assurer qu'une cartographie des processus est formalisée S'assurer que la cartographie est exhaustive et complète	Omission de processus Incomplétude de la description des processus (Flux entrants & sortants, ressources & moyens, SI, participation aux résultats)	Cartographie des processus formalisée	Si les cartographies sont mal élaborées et incomplètes, la stratégie de continuité et les dispositifs de continuité qui se basent sur ces cartographies seront également inadaptés ou insuffisants	Formalisation d'une cartographie des processus exhaustive et complète	Revue de la cartographie des processus
		S'assurer qu'une cartographie des risques est formalisée S'assurer que la cartographie est exhaustive et pertinente S'assurer que les impacts et probabilités d'occurrence ont été correctement estimés	Omission de risques (risques globaux et risques attachés à chaque processus) Identification des impacts incomplète ou non pertinente Mauvaise évaluation de la criticité des risques (occurrence & impact)	Cartographie des risques		Formalisation d'une cartographie des risques exhaustive, complète et pertinente	Revue de la cartographie des risques Etude de la méthode d'élaboration de la cartographie (implication des opérationnels, appui de consultants externes, utilisation de référentiels et d'outils spécifiques...) Revue des méthodes d'estimation des impacts et probabilités d'occurrence

		S'assurer qu'une analyse des impacts d'interruption est réalisée pour toutes les activités de l'organisation S'assurer que l'analyse des impacts d'interruption tient compte de tous les risques S'assurer que l'analyse des impacts d'interruption est pertinente	Mauvaise analyse des impacts Omission d'activités Omission de risques	Analyses des impacts d'une interruption d'activité formalisées	Non pertinence de la stratégie de continuité et des dispositifs de continuité : Inadéquation aux besoins réels, inefficacité ou efficience imparfaite	Conduite d'une analyse des impacts d'interruption pour chaque activité vis-à-vis des risques relatifs à cette activité et à l'organisation Formaliser pour chaque activité le DMIA et le PMDT	Revue de la méthode d'estimation des impacts d'interruption Rapprochement des analyses d'impacts d'interruption des cartographies des processus et des risques Revue des impacts identifiés
		S'assurer que les services en amont et en aval de l'organisation ainsi que les acteurs qui les fournissent ont été correctement identifiés S'assurer que les risques associés ont été correctement définis et analysés (en termes d'impact sur l'organisation et de probabilité d'occurrence) S'assurer de la correcte prise en compte et analyse des dispositifs de continuité d'activité et de maîtrise des risques en place chez les acteurs externes concernés	Identification incomplète ou non pertinente des services en amont et en aval de l'organisation et des acteurs qui les fournissent Mauvaise cartographie des risques associés (omission de risques, mauvaise identification des impacts sur l'organisation et de la probabilité d'occurrence) Non prise en compte ou mauvaise analyse des dispositifs de continuité d'activité et de maîtrise des risques en place chez les acteurs externes	Définition de la criticité des services en amont et en aval de l'organisation Cartographie des services en amont et en aval de l'organisation, et des risques associés	Défaillance de la continuité d'activité de l'organisation découlant de la défaillance de ses partenaires externes Gaspillage de ressources pour la mise en place de dispositifs de continuité déjà en place chez les partenaires externes	Identification des services en amont et en aval de l'organisation et les acteurs qui les fournissent Cartographie des risques associés à ces services Analyse des impacts potentiels sur l'organisation et de leur criticité Analyse des dispositifs de continuité d'activité et de maîtrise des risques en place chez les acteurs externes concernés	Revue de la cartographie des services en amont et en aval de l'organisation avec les acteurs qui les fournissent Revue de la méthode d'établissement de cette cartographie (implication des opérationnels, appui de consultants externes, utilisation de référentiels et d'outils spécifiques...) Revue de la cartographie des risques associés et de sa méthode d'élaboration, notamment les analyses d'impacts sur l'organisation et de la probabilité d'occurrence Revue des analyses des dispositifs de continuité d'activité et de maîtrise des risques des acteurs externes concernés
		S'assurer de la bonne prise en compte des dispositifs existants (identification et analyse) S'assurer de la bonne détection des failles dans les dispositifs existants	Absence ou insuffisance de la prise en compte des dispositifs existants Mauvaise analyse des dispositifs Mauvaise identification des failles dans les dispositifs existants	Analyse des dispositifs de maîtrise des risques déjà existants en interne formalisée	Défaillance de la continuité d'activité liée aux risques non maîtrisés par les autres dispositifs de maîtrise des risques Gaspillage de ressources pour la mise en place de dispositifs associés à des risques déjà maîtrisés	Analyse des dispositifs de maîtrise des risques déjà existant dans l'organisation pour prise en compte dans le PCA	Revue de la cartographie des dispositifs existants et des failles, et rapprochement de celle-ci avec les travaux du Contrôle Interne et du Management des Risques Revue de la méthode d'analyse des dispositifs existants (implication des opérationnels, appui de consultants externes, utilisation de référentiels et d'outils spécifiques...)
		S'assurer que les objectifs stratégiques de l'organisation sont pris en compte pour l'identification des activités critiques et la stratégie de continuité	Absence ou mauvaises définition des objectifs stratégiques de l'organisation par la DG Engagement de la DG insuffisante dans la démarche PCA	Consultation de la Direction Générale dans le cadre de l'identification des activités critiques	Démarche PCA non légitimée auprès du personnel Démarche PCA déconnectée des objectifs stratégiques de l'organisation Allocation de ressources insuffisantes à la démarche	Consultation et respect des directives et orientations de la DG en termes d'objectifs stratégiques et d'identification des activités critiques	Consultation des échanges entre la gouvernance du PCA et la DG (e-mails, comptes-rendus de réunion, note de cadrage…)

		S'assurer que les obligations règlementaires relatives à la continuité d'activité sont connues et prises en compte pour l'identification des activités critiques et la stratégie de continuité	Méconnaissance de la règlementation en vigueur (absence ou insuffisance de veille règlementaire) Absence ou insuffisance de la prise en compte de ces obligations (manque de communication entre le service juridique et l'équipe PCA, manque de sensibilisation des acteurs aux problématiques juridiques...)	Prise en compte des obligations règlementaires	Non-conformité du dispositif de continuité d'activité avec les obligations règlementaires liées (sanctions, dégradation de l'image de l'organisation…)	Prise en compte et respect des obligations règlementaires en termes de continuité d'activité auxquelles est soumise l'organisation	Revue de la méthodologie de veille règlementaire Consultation des échanges entre le service juridique et l'équipe PCA
		S'assurer que les activités critiques ont été correctement identifiées S'assurer que les activités critiques sont hiérarchisées en fonction de leur niveau de criticité de manière pertinente	Non prise en compte des cartographies des processus et des risques, des analyses d'impacts d'interruption d'activité, de la criticité des services en amont et en aval de l'organisation, de l'analyse des dispositifs de maîtrise des risques déjà existants, des objectifs stratégiques de la DG et des obligations règlementaires pour l'identification des activités critiques et de leur niveau de criticité	Identification des activités critiques et du niveau de cette criticité formalisées	Non pertinence de la stratégie de continuité et des dispositifs de continuité d'activité, ne permettant pas d'assurer la continuité d'activité des activités critiques de l'organisation de manière satisfaisante	Liste des activités critiques hiérarchisées en fonction de leur niveau de criticité, pour lesquelles il est essentiel de mettre en place un PCA	Revue de la liste d'activité critique et de leur hiérarchisation Revue de la méthode d'identification des activités critiques et de leur hiérarchisation
	Elaboration de la stratégie de continuité	S'assurer que les activités critiques ont bien été identifiées et classifiées dans l'ordre de leur criticité S'assurer que les besoin en continuité associés aux activités critiques sont correctement évalués	Absence ou mauvaise classification des activités critiques Mauvaise identification des besoins en continuité correspondants	Définition des besoins en continuité des métiers formalisée	Dispositifs de continuité d'activité inadaptés aux besoins ou inopérants C'est le cœur de la démarche PCA, auquel les autres composantes viennent en support. S'ils ne sont pas pertinents, c'est toute la démarche qui sera caduque	Classification des activités critiques par ordre de criticité et définition des besoins en continuité associés	Revue de la liste des activités critiques et de leur hiérarchisation Revue de la méthode d'identification des activités critiques et de leur hiérarchisation Revue de la liste des besoins en continuité en fonction des activités critiques et de la méthode de détermination de ces besoins
		S'assurer que les solutions de continuité envisagées sont cohérentes avec les besoins de continuité	Listing non exhaustif des solutions envisagées Solutions de secours non adaptés aux besoins de continuité	Elaboration des solutions PCA métiers		Listing des solutions de secours correspondantes aux besoins en continuité définis	Revue de la méthode d'élaboration des solutions Revue des solutions proposées en les rapprochant des besoins en continuité et des objectifs de continuité
		S'assurer que les ressources et moyens nécessaires aux solutions ont été correctement identifiés	Mauvaise estimation des ressources nécessaires à la mise en place des solutions de continuité Incohérence entre les besoins exprimés et les ressources dont dispose l'organisation	Définition des moyens nécessaires aux solutions de continuité	Besoins sous-évalués : Allocation de ressources insuffisantes à la démarche PCA Besoins surévalués : Non validation des dispositifs par la DG	Identification des ressources humaines et matérielles nécessaires à la mise en place des solutions de secours	Revue de la méthode d'estimation des besoins en ressources Revue des besoins en ressources exprimés, en les rapprochant des besoins en continuité et des ressources disponibles dans l'organisation

		S'assurer que l'organisation à bien mis en place un PSI complet et adapté aux besoins opérationnels de l'organisation S'assurer que le PSI prend en compte les dimensions de confidentialité et de sécurité informatique S'assurer qu'un dispositif pertinent de continuité de fonctionnement pour les données et applicatifs critiques est prévu et formalisé S'assurer qu'un dispositif pertinent de continuité de fonctionnement pour les principaux systèmes de télécommunications est prévu et formalisé	Mauvaise identification des applications et bases de données critiques Mauvaise identification des systèmes de télécommunication principaux Absence ou mauvaise coordination et prise en compte des besoins des opérationnels Absence ou non pertinence de la confidentialité et de la sécurité informatique Absence de contractualisation de la continuité informatique entre les opérationnels et la DSI	Mise en place d'un PSI formalisé	Non disponibilité des outils et supports nécessaires au déploiement des solutions de continuité des métiers, donc impossibilité de déployer les dispositifs Défaillance de la continuité d'activité de l'organisation	Elaboration d'un plan de secours informatique pour les applicatifs critiques, l'accès aux bases essentielles et des systèmes de télécommunication principaux	Revue du mode de détermination des applications, bases de données et systèmes de télécommunication critiques, en particulier la prise en compte des besoins des opérationnels Revue des applications, bases de données et systèmes de télécommunications identifiés comme critiques et les rapprocher des besoins en continuité et en ressources exprimés par les opérationnels pour les PCA métiers Revue des dispositifs de sécurisation des données et des systèmes d'information
		S'assurer de la bonne identification des besoins en services supports minimaux de l'organisation	Mauvaise identification des besoins en services support Absence ou mauvaise définition et prise en compte des besoins en services exprimés par les opérationnels Solutions des PCA services supports mal conçues ou inadaptées aux besoins	Elaboration des solutions PCA services supports		Identification des besoins en services support minimaux Elaboration de solutions de continuité des services supports adaptées à ces besoins	Revue de la méthode de recensement des besoins en continuité des services supports Revue des besoins en continuité des services supports exprimés et les rapprocher des besoins en ressources exprimés par les opérationnels pour les PCA métiers Revue des solutions des PCA services support et vérifier leur cohérence avec les besoins en continuité des services supports
		S'assurer de la bonne définition des besoins en continuité de l'organisation vis-à-vis de ses partenaires et de la sollicitation de ces derniers sur ces points S'assurer de l'implication des partenaires externes dans la stratégie de continuité d'activité et de la contractualisation de leurs engagements	Absence de sollicitation des partenaires sur ces problématiques Absence ou insuffisance de sensibilisation ou d'implication de la part des partenaires Refus de coopération des prestataires Mauvaise détermination des besoins en continuité de l'organisation vis-à-vis de ses partenaires Absence ou mauvaise contractualisation des engagements de continuité pris par les partenaires	Prise en compte de la continuité d'activité des partenaires de l'organisation		Requête de mise en place de PCA chez les partenaires essentiels de l'organisation	Revue de la méthode de détermination des besoins en continuité vis-à-vis des partenaires Revue des besoins en continuité des partenaires exprimés, et les rapprocher des besoins exprimés par les opérationnels pour les PCA métiers Revue des contrats avec les partenaires de l'organisation autour de la continuité d'activité

		S'assurer qu'une articulation entre les différentes composantes du PCA et une organisation globale existe S'assurer de la cohérence des différentes composantes entre elles	Absence ou mauvaise articulation des composantes du PCA entre elles	Proposition d'une organisation globale du PCA formalisée	Absence de cohérence globale et de coordination entre tous les dispositifs, mauvaise circulation des flux et goulots d'étranglement, impossibilité de déployer les processus simultanément	Révision globale des composantes du PCA et de leur articulation entre eux	Revue des contrôles de cohérence et de schémas des flux réalisés sur l'articulation des différentes composantes du PCA entre elles Vérifier qu'une organisation globale du PCA est prévue, et en évaluer la pertinence
		<u>Dans le cas des structures complexes :</u> S'assurer que la stratégie de continuité du groupe est correctement déployée et appliquée dans les filiales S'assurer que les dispositifs sont correctement adaptés aux spécificités de la filiale et de son activité	Mauvaise intégration des filiales à la stratégie de continuité Mauvaise coordination entre la filiale et la maison mère Absence ou mauvaise application des prérogatives de la maison mère en ce qui concerne les PCA Absence ou mauvaise mutualisation des ressources et moyens	Déploiement du dispositif de continuité d'activité à l'ensemble du groupe (maison mère et toutes les filiales)	Défaillance de la continuité d'activité liée à la défaillance de filiales interdépendantes Gaspillage de ressources lié à la non mutualisation des dispositifs entre les filiales	Intégration des filiales dans la stratégie de continuité d'activité Déploiement du dispositif de continuité dans l'ensemble des filiales du groupe	Revue de la stratégie de continuité définie par les filiales, et vérifier son adéquation avec la stratégie définie par le groupe
		S'assurer que des mesures préventives sont prévues dans les nouveaux projets pour diminuer la probabilité de survenance de sinistres	Absence de mesure de prévention Mauvaise estimation des risques courus par l'organisation Mesures de prévention inefficaces Absence ou mauvaise intégration de la démarche PCA lors du lancement de nouveaux projets	Intégration de la dimension préventive du PCA dans les nouveaux projets	Gaspillage de ressources lié à la mise en place ultérieure de dispositifs de continuité d'activité non anticipés	Réflexion sur la continuité d'activité systématique lors du développement de chaque nouveau projet de l'organisation Lancement ou renforcement de mesures de prévention pour diminuer la probabilité de survenance de sinistres	Revue des dossiers des projets lancés postérieurement à la démarche PCA de l'organisation, et vérification de l'intégration des aspects de continuité d'activité
	Validation de l'étape	S'assurer que la définition et hiérarchisation des activités critiques dans le cadre du projet PCA sont bien validées par les organes de gouvernance du projet PCA ainsi que par la Direction Générale	Absence de validation préalable des propositions par le pilotage du projet PCA Désintérêt de la direction pour le projet Abandon ou mise en attente du projet	Validation des activités critiques identifiées et de la stratégie de continuité formalisée	Mise en attente du projet Absence d'allocation de ressources Incertitude quant à la conformité règlementaire du dispositif	Validation de la définition des activités critiques et de la stratégie de continuité d'activité par la gouvernance du PCA et la DG	Consulter la traçabilité des échanges entre les opérationnels concepteurs de la stratégie de continuité et des solutions PCA et la gouvernance du projet PCA et la Direction Générale Consulter les ordres du jour et les comptes-rendus de réunion des organes de gouvernance du PCA autour de la validation des propositions
Etape 3 : Etudier et choisir les solutions envisageables	Etude de faisabilité et chiffrage des solutions	S'assurer que la faisabilité des solutions a été vérifiée d'un point de vue technique, humain et matériel S'assurer de leur conformité au regard des normes et règlementations applicables	Absence ou mauvaise réalisation de l'étude de faisabilité technique des solutions Faisabilité technique difficile voire impossible Moyens humains et matériels inadaptés au déploiement	Réalisation d'une étude de faisabilité des solutions envisagées sur la base de critères techniques	Défaillance de la continuité d'activité liée à l'impossibilité de déployer les dispositifs de continuité	Etude de la faisabilité technique des solutions envisagées : Moyens humains, moyens matériels, savoirs-faire, et conformité des solutions envisagées avec la réglementation en	Revue de l'étude de faisabilité technique des solutions

			des solutions Solutions non conformes aux normes ou à la règlementation applicables			vigueur	
		S'assurer que la faisabilité organisationnelle des solutions a été vérifiée S'assurer que les solutions envisagées peuvent être intégrées à l'organisation	Absence ou mauvaise réalisation de l'étude de faisabilité organisationnelle des solutions Solutions difficilement intégrables à l'organisation Mise en place des solutions trop lourde de réorganisation interne	Réalisation d'une étude de faisabilité des solutions envisagées sur la base de critères organisationnels		Etude de la faisabilité organisationnelle : Capacité à intégrer les solutions à l'organisation actuelle	Revue de l'étude de faisabilité organisationnelle des solutions
		S'assurer que l'évaluation financière des solutions a été correctement réalisée S'assurer que les solutions envisagées sont faisables d'un point de vue financier	Absence ou mauvaise réalisation de l'évaluation financière Faisabilité financière difficile Mauvaise budgétisation des solutions	Réalisation d'une étude de faisabilité des solutions envisagées sur la base de critères financiers		Etude de la faisabilité financière des solutions et budgétisation	Revue des estimations financières des solutions
	Evaluer la pertinence des solutions	S'assurer que les solutions envisagées permettent de maîtriser les risques et de garantir la continuité puis la reprise des activités en cas de survenance de sinistre S'assurer que les coûts de déploiement des solutions ne sont pas supérieurs aux coûts d'interruption	Absence ou mauvaise évaluation de la pertinence des solutions Evaluation de la pertinence des solutions envisagées sans prise de connaissance de leur faisabilité au préalable Moyens et ressources nécessaires au déploiement des solutions plus importants que les coûts d'interruption	Réalisation d'une étude de la pertinence des solutions envisagées	Dispositifs de continuité d'activité inadaptés : Dispositifs inopérants, ne répondant pas aux attentes de la DG ou impliquant des coûts supérieurs aux coûts d'une interruption d'activité	Etude de la pertinence des solutions envisagées à travers le degré de réponse aux objectifs de continuité et rapprochement du coût d'une interruption	Revue de l'étude de pertinence des solutions
	Choix des solutions	S'assurer que les choix de solutions de continuité sont adaptés à l'organisation et pertinents, et qu'ils répondent aux objectifs et besoins en continuité S'assurer que les solutions retenues sont en cohérence avec les études préalables de faisabilité technique, organisationnelle et financière	Absence ou mauvaise formalisation des solutions retenues, en particulier lorsque plusieurs solutions différentes sont proposées pour un même métier Solutions de continuité choisies inadaptées ou non faisables	Choix des solutions à déployer formalisé	Défaillance de la continuité d'activité liée à une confusion sur les solutions à déployer lors de la survenance d'un sinistre, ou au déploiement d'une solution non faisable ou non pertinente	Choix des solutions de continuité retenues à l'issue des études de faisabilité et de pertinence	Revue du mode de sélection des solutions Revue des solutions choisies en les rapprochant des études de faisabilité, d'estimation financière et de pertinence qui les concernent ainsi que de la stratégie de continuité
Etape 4 : Mettre en place une base documentaire		S'assurer que les éléments liés à la stratégie de continuité sont correctement formalisés, documentés et archivés	Absence ou mauvaise formalisation, documentation et conservation des documents relatifs au PCA de l'organisation	Mise en place d'une base documentaire dédiée à la documentation du PCA	Perte, destruction, corruption ou vol d'informations stratégiques et/ou confidentielles Difficulté accrue pour maintenir et mettre à jour le PCA Non-respect ou absence	Formalisation, documentation et conservation de tous les éléments qui composent les PCA	Vérifier la pertinence du mode d'archivage des documents du PCA, et notamment sa sécurité et sa confidentialité, ainsi que la désignation des personnes qui en sont responsables Vérifier l'exhaustivité et la qualité de son contenu

					de preuve du respect des obligations règlementaires		
Etape 5 : Politique de communication	Communication Interne	S'assurer de l'existence et de la qualité d'une politique de communication en interne auprès des acteurs du PCA et de l'ensemble des collaborateurs S'assurer de la correcte mise en application de la politique de communication interne S'assurer que la communication interne est prévue à la fois avant, pendant et après la survenance d'un sinistre	Absence de définition et formalisation d'une politique de communication interne Politique de communication interne inadaptée ou non pertinente Non-respect de la politique de communication interne Absence ou mauvais déploiement de ressources et moyens associés à la communication interne	Formalisation d'une stratégie de communication interne dans le cadre des PCA Mise en place de dispositifs de communication interne	Défaillance de la continuité d'activité liée à la mauvaise réaction du personnel dans l'urgence ou à la panique de celui-ci Transition et retour à la normale difficile Absence de retour d'expérience sur la continuité d'activité : Démotivation du personnel et non amélioration du dispositif	Définition et application d'une politique de communication interne	Revue de la politique de communication interne Consultation des messages effectivement diffusés et leur mode de diffusion, et vérifier leur cohérence avec la politique de communication interne
	Communication Externe	S'assurer de l'existence et de la qualité d'une politique de communication en externe auprès des parties prenantes S'assurer de la correcte mise en application de la politique de communication externe S'assurer que la communication externe est prévue à la fois avant, pendant et après la survenance d'un sinistre	Absence de définition et formalisation d'une politique de communication externe Politique de communication externe inadaptée ou non pertinente Non-respect de la politique de communication externe Absence ou mauvais déploiement de ressources et moyens associés à la communication externe	Formalisation d'une stratégie de communication externe dans le cadre des PCA Mise en place de dispositifs de communication externe	Dégradation de l'image de l'organisation Perte potentielle de clients	Définition et application d'une politique de communication externe auprès des partenaires, des clients et des investisseurs	Revue de la politique de communication externe, et notamment du ou des porte-paroles désignés Consultation des messages effectivement diffusés et leur mode de diffusion, et vérifier leur cohérence avec la politique de communication externe
	Confidentialité	S'assurer de la bonne classification des informations relatives au PCA selon les différents niveaux de confidentialité S'assurer de la sécurisation des informations confidentielles liées au PCA de l'organisation (système d'informations, base de données et base documentaire)	Absence ou mauvaise classification des informations liées au PCA Absence ou mauvaise sécurisation des systèmes d'information, des bases de données et de la base documentaire du PCA Absence ou mauvaise sensibilisation du personnel sur les problématiques de confidentialité du PCA	Formalisation d'une stratégie de gestion de la confidentialité des informations relatives aux PCA Mise en place de dispositifs visant à garantir cette confidentialité	Perte, destruction, corruption ou vol des informations relatives au PCA	Classification des informations liées aux PCA selon trois niveaux de confidentialité Sécurisation des systèmes d'information et des données Sensibilisation du personnel à la confidentialité du PCA	Revue des différents niveaux de classification de confidentialité existants dans l'organisation Revue du mode de classification des informations relatives au PCA Evaluation des dispositifs de sécurisation des systèmes d'information, bases de données et base documentaire du PCA Test de la sécurisation des informations via une simulation d'intrusion pour vol ou endommagement des informations

3.3.2 Le déploiement du PCA

Etapes de mise en place d'un PCA et d'une gestion de crise : Composantes du Contrôle Interne		Finalités : Objectifs de Contrôle Interne Objectifs d'Audit	RISQUES			Bonnes pratiques de Contrôle Interne	Techniques d'audit
			Facteurs (Scénarios d'empêchement)	Points de contrôle	Impacts		
Gestion de crise	Constitution d'une cellule de crise	S'assurer de l'existence d'une cellule de crise et de l'attention portée à sa constitution S'assurer de la nomination d'un responsable de la mise en en place de la cellule de crise, qui en sera le pilote	Absence ou mauvais choix du pilote de la cellule de crise Non implication du pilote de la cellule de crise Constitution de la cellule de crise non pertinente, mauvaise identification de ses membres	Cellule de crise constituée	Réalisation des tâches non optimales du fait de l'absence de responsables identifiés ou de carences de compétences Manque de légitimité en interne	Nomination de la personne chargée de la mise en place de la cellule de crise en accord avec le Comité de Pilotage Constitution de la cellule de crise	Revue du mode de désignation du pilote de la cellule de crise et de constitution de celle-ci Evaluation de la pertinence du choix du pilote et des membres qui composent la cellule de crise
	Dispositifs de veille, de remontée et de gestion des incidents	S'assurer de la bonne sélection des indicateurs d'activité à surveiller S'assurer de la surveillance des indicateurs d'activité permettant de détecter et d'anticiper la survenance d'un sinistre S'assurer de l'existence et de l'efficience d'un dispositif de remontée et de gestion des incidents S'assurer de la traçabilité de la veille réalisée, ainsi que de la remontée et du traitement des incidents	Absence ou mauvaise surveillance des indicateurs d'activité permettant de détecter et d'anticiper la survenance d'un sinistre Absence ou mauvaise définition et formalisation d'un dispositif de remontée et de traitement des incidents Absence ou mauvaise traçabilité de la veille réalisée	Dispositif de veille, de remontée et de gestion des incidents formalisé Indicateurs d'activité identifiés et suivis	Non traitement des incidents mineurs qui deviennent systématiquement des sinistres de grande ampleur Mauvaise réactivité, impacts subis plus importants Vulnérabilité accrue de l'organisation aux sinistres	Suivi et surveillance des indicateurs d'activité permettant de détecter et d'anticiper la survenance d'un sinistre Dispositif de remontée et gestion des incidents formalisé Documentation et traçabilité de la veille réalisée	Revue des indicateurs d'activité retenus Revue du dispositif de veille de ces indicateurs prévu Vérifier l'effective surveillance de ces indicateurs réalisés (documentation de la surveillance : tableaux de bord…) Revue du dispositif de remontée et de gestion des incidents Vérifier et évaluer la qualité de la traçabilité de la veille des indicateurs, ainsi que de la remontée et du traitement des incidents
	Dispositifs d'alerte et d'escalade	S'assurer de l'existence d'un dispositif d'alerte et d'escalade performant permettant de déclencher le PCA en cas de besoin et d'informer les autorités compétentes S'assurer d'une allocation pertinente des ressources et moyens au dispositif d'alerte et d'escalade S'assurer de la traçabilité des alertes et de l'escalade	Dispositifs d'alerte et d'escalade inexistants, défaillants ou non pertinents Déficience du dispositif d'information des autorités compétentes Absence ou mauvaise traçabilité de la remontée des incidents	Dispositif d'alerte et d'escalade formalisé	Mauvaise réactivité de l'organisation, impacts subis plus important lors de la survenance d'un sinistre Vulnérabilité accrue de l'organisation aux sinistres	Dispositifs d'alerte et d'escalade en cas de survenance d'un sinistre formalisés Information des autorités compétentes lorsque la règlementation l'impose Documentation et traçabilité de la remonté des incidents, ainsi que des alertes et escalades	Revue du dispositif d'alerte et d'escalade prévu (test de cheminement) Test effectif du dispositif via une simulation de la survenance d'un sinistre Vérifier et évaluer la qualité de la traçabilité des alertes et de l'escalade
	Gestion de la crise et de la communication	S'assurer que les dispositifs de gestion de crise prévoient de manière opérante la transition vers le mode dégradé, l'accompagnement et le soutien aux opérationnels dans le déclenchement des procédures de continuité et la gestion des imprévus	Absence ou mauvais accompagnement de la transition vers le mode dégradé Absence ou mauvais accompagnement des opérationnels dans le déclenchement des procédures de continuité	Dispositif de gestion de la crise opérationnel et formalisé	Absence de soutien aux opérationnels dans le déploiement des PCA Gestion des imprévus non optimale Absence de coordination globale	Transition vers le mode dégradé Déclenchement des procédures de continuité et accompagnement et soutien aux opérationnels Gestion des imprévus	Revue des dispositifs de gestion de crise et test de leur efficacité et de leur efficience théorique Audit post crise pour évaluer l'utilisation des dispositifs qui avaient été prévus et le niveau de maîtrise de la crise

			Incapacité à réagir aux imprévus				
		S'assurer que les informations relatives à la crise sont communiquées de manière adéquate à la fois en interne et en externe S'assurer que le personnel est informé de ses rôles et responsabilités et reçoit des consignes en cas de crise et d'enclenchement du PCA S'assurer qu'un journal de bord est correctement formalisé afin de garantir la traçabilité et préparer le retour d'expérience	Communication de crise non organisée et inopérante ou non optimale Personnel non informé et non guidé à travers la gestion de crise et le déploiement des procédures de continuité Absence ou mauvaise formalisation d'un journal de bord	Dispositif de gestion de la communication de crise opérationnel et formalisé	Panique et désorganisation Dégradation de l'image de l'organisation Manque de traçabilité des évènements pour un retour d'expérience pertinent	Pilotage de la communication de crise via l'information interne et externe, et la distribution de consignes au personnel lors de l'enclenchement du PCA Tenue d'un journal de bord de crise pour la traçabilité et la préparation du retour d'expérience	Revue du plan de communication de crise Test effectif du plan de communication de crise via la simulation de la survenance d'un sinistre Evaluation post-crise du journal de bord formalisé Audit post-crise sur la communication de crise réalisée
	Sortie de crise et retour à une situation normale	S'assurer de la surveillance de l'évolution de la situation de la crise pour déclenchement du PRA, puis accompagnement de ce déclenchement S'assurer de la réalisation d'un retour d'expérience de la crise utile et pertinent	Absence de déclenchement du PRA Absence ou mauvais suivi de l'évolution de la situation de la crise pour déclenchement du PRA au moment opportun Absence ou mauvais accompagnement de la transition vers la reprise d'activité puis un retour à la situation normale Absence ou non pertinence et inutilité du retour d'expérience sur la crise	Dispositif d'accompagne-ment à la sortie de crise prévu et formalisé	Sortie de crise moins rapide, dommages subis plus importants Absence d'amélioration du dispositif de continuité d'activité à l'issue de la crise	Déclenchement du plan de reprise d'activité vers un retour à la normale Retour d'expérience sur la crise	Revue du dispositif de surveillance de l'évolution de la situation de la crise et de déclenchement de la reprise d'activité Audit post-crise pour vérifier le correct déclenchement du PRA Evaluation de la qualité du retour d'expérience de la crise
Logistique de crise	Site de repli	S'assurer de l'existence d'un site de repli prêt pour accueillir les activités critiques de l'organisation fonctionnant en mode dégradé	Absence de site de repli prévu Site de repli non prêt Site de repli incapable d'accueillir les activités critiques	Site de repli prévu et opérationnel	Impossibilité de déployer les dispositifs de continuité d'activité due à l'absence ou à l'indisponibilité du matériel nécessaire, ou à l'impossibilité d'y avoir accès Déploiement des dispositifs non optimal ou plus long, du fait de la difficulté d'accès au matériel nécessaire, avec par conséquent des dommages subis plus importants	Site alternatif au site de travail principal, prêt pour accueillir les activités critiques fonctionnant en mode dégradé	Vérifier l'existence d'un site de repli et en évaluer la préparation, vérifier qu'il peut être opérationnel rapidement en cas de survenance d'un sinistre, notamment en termes d'équipements et d'infrastructures, d'alimentation en énergie et de systèmes d'information Vérifier que le site de repli est en mesure d'accueillir les activités critiques de l'organisation Test effectif du site de repli via une simulation de sinistre
	Matériel de secours	S'assurer de l'existence de matériel de secours prêt à prendre le relai pour assurer le niveau de service minimum des activités critiques de l'organisation en cas de défaillance de l'outil de travail habituel	Absence ou insuffisance du matériel de secours pour permettre d'assurer le niveau de service minimum des activités critiques en cas de défaillance de l'outil de travail habituel Matériel de secours non prêt	Matériel de secours prévu et opérationnel		Matériel de secours prêt à prendre le relais en cas de défaillance de l'outil de travail habituel (moyens de télécommunications, systèmes d'information, alimentation en énergie alternative, matériel de	Vérifier l'existence de matériel de secours et en évaluer la préparation, vérifier qu'il peut être opérationnel rapidement en cas de survenance d'un sinistre Vérifier que le matériel de secours est suffisant pour assurer le niveau de service minimum des activités critiques de l'organisation

						production…)	Test effectif du matériel de secours via une simulation de la survenance d'un sinistre
	Transport	S'assurer de la prévision d'une logistique de crise, visant en particulier à assurer le transport du personnel des activités critiques vers le site de repli	Absence de plan de logistique de crise, en particulier le transport du personnel vers le site de repli Incapacité de déplacer les activités critiques vers le site de repli	Logistique de crise (notamment le transport vers le site de repli) prévue, opérationnelle et formalisée		Logistique de crise pour le déménagement vers le site de repli, notamment les solutions de transport du personnel	Revue de la logistique de crise prévue Test de la logistique de crise via la simulation d'un sinistre Audit post-crise pour évaluer l'efficacité et l'efficience de la logistique de crise déployée
Protection et sécurité du personnel		S'assurer que la sécurité du personnel est garantie en situation de crise	Mesures et dispositifs de sécurité et de protection du personnel inexistants, insuffisants ou non pertinents	Mesures et dispositifs de sécurité et de protection du personnel opérationnels et formalisés	Dégâts humains, privant l'organisation de personnel Dégradation de l'image de l'organisation Sanctions	Garantie de la sécurité du personnel en cas de crise par un ensemble de mesures et dispositifs prévus et formalisés en amont de la survenance d'une crise	Revue des mesures et dispositifs de sécurité et de protection du personnel prévu Test effectif des dispositifs via la simulation d'une crise Audit post-crise afin de mesurer l'efficacité des dispositifs déployés et les éventuelles atteintes à la sécurité dont ont été victimes les salariés
Implication des partenaires indispensables		S'assurer de la correcte contractualisation des prestations de secours avec les prestataires S'assurer qu'un interlocuteur spécifique chez les prestataires de secours a été identifié	Absence ou mauvaise formalisation des contrats de prestation de services de secours Absence ou mauvaise identification des interlocuteurs au sein des partenaires	Contrats formalisés avec les prestataires de secours	Impossibilité de déployer les dispositifs de continuité d'activité due à l'absence ou l'indisponibilité des ressources et moyens nécessaires	Formalisation des contrats spécifiques qui prévoient le recours à des prestataires de secours pour le déploiement du PCA Identification des interlocuteurs au sein des prestataires concernés	Revue des contrats avec les prestataires de secours Consultation des échanges entre l'organisation et les prestataires pour vérifier la constance des interlocuteurs
Information et formation des acteurs impliqués	Identification des acteurs à former	S'assurer que les acteurs concernés par le PCA ont été correctement identifiés	Absence ou mauvaise identification des acteurs concernés par les PCA	Acteurs concernés par le PCA identifiés	Panique, désorganisation et réactivité du personnel non optimale en cas de survenance d'une crise Dommages subis plus importants, vulnérabilité accrue de l'organisation aux sinistres Manque d'implication, de motivation et d'appropriation du dispositif par le personnel	Identification des acteurs concernés par les PCA pour les informer et les former	Revue de la méthode d'identification des acteurs Revue des acteurs identifiés et en rapprocher la liste des procédures PCA métiers
	Organisation de la formation	S'assurer que les bonnes personnes sont désignées pour dispenser les formations au reste des acteurs PCA S'assurer de l'organisation optimale des formations PCA	Absence de formation des acteurs du PCA Absence ou mauvaise identification des personnes apte à former les acteurs du PCA Absence de personnel capable de former les collaborateurs aux PCA Organisation des formations au PCA non optimale	Dispositif de formation organisé et formalisé Formateurs désignés		Identification des personnes qui ont une connaissance suffisante du dispositif de continuité pour former les collaborateurs concernés par le PCA Organisation optimale de la formation (groupes réduits, par métiers…)	Revue des personnes sélectionnées pour dispenser les formations aux autres acteurs du PCA Revue de l'organisation des formations et vérification de leur optimisation
	Contenu de la formation	S'assurer que la formation couvre les points essentiels du dispositif	Formation incomplète ou inadéquate	Programme de formation formalisé et approuvé		Couverture des points essentiels par la formation (stratégie de continuité, présentation du site de repli,	Revue du contenue de la formation dispensée

						rémunération associée au PCA, procédures liées au service ou métier, vie du PCA…)	
	Exercices	S'assurer que des exercices pratiques complet et pertinente viennent compléter la formation théorique sur le PCA pour l'ensemble des acteurs concernés	Absence d'exercices de préparation Exercices non pertinents ou incomplets Non-participations de tous les acteurs concernés aux exercices	Programme d'exercices pratiques formalisé et approuvé		Organisation d'exercices pratiques et mises en situation de crise pour compléter la formation théorique	Vérifier la réalisation d'exercices pratiques en complément de la formation théoriques Evaluer la complétude et la pertinence des exercices Vérifier que tous les acteurs concernés par le PCA participent aux exercices
Implication et support de la Direction Générale		S'assurer que la Direction Générale est impliquée dans le projet PCA de manière suffisante et adéquate	Absence ou insuffisance du soutien et de l'implication de la Direction Générale dans le projet PCA Non mise à disposition des ressources et moyens pour le déploiement des PCA Absence ou insuffisance de l'intervention de la Direction Générale en période de crise Inadéquation de l'intervention de la Direction Générale	Implication et support de la Direction Générale (transmission de messages, sensibilisation des collaborateurs, allocation de ressources…)	Manque de légitimité de la démarche en interne, manque d'implication et de motivation des collaborateurs Insuffisance des ressources allouées au dispositif	Mobilisation de la Direction Générale depuis le commencement du projet PCA jusqu'à son déploiement, et son intervention en tant que support en période de crise	Vérification du déploiement de ressources et moyens suffisants pour le PCA Consultations des messages émanant de la Direction Générale concernant le PCA Entretien avec la Direction Générale pour mesurer sa sensibilisation et son implication envers le PCA de l'organisation
Mallettes de crise		S'assurer de la détention par tous les responsables de PCA métiers ou services supports de mallettes de crise opérationnelles et disponibles	Absence de mallettes de crise Mallettes de crise incomplètes Mallettes de crise non à jour ou non opérationnelles Contenu des mallettes de crise inadapté Mallettes de crise non disponibles en cas de besoin Mallettes de crise non détenues par tous les responsables de PCA métiers ou services support Méconnaissance de l'existence des mallettes de crise par les acteurs concernés	Mallettes de crise opérationnelles détenues par les responsables de PCA métiers ou services supports	Réactivité de l'organisation et déploiement des dispositifs de continuité d'activité non optimisés du à un manque de matériel d'urgence Dommages subis plus importants	Mise en place de mallettes de crise pour les responsables des PCA métiers et services support	Vérifier l'existence et la disponibilité de mallettes de crise dans l'organisation Vérifier que chaque responsable de PCA métier ou service support détient une mallette de crise Evaluation de la pertinence du contenu des mallettes de crise Vérifier que les mallettes de crise sont à jour et opérationnelles
Premier test technique du PCA et validation	Organisation et conception du test	S'assurer qu'un premier test technique du PCA est réalisé, et qu'il porte sur l'ensemble de ses composantes	Absence de réalisation d'un premier test technique du PCA Premier test technique du PCA incomplet, n'incluant pas toutes les composantes de celui-ci Conception et organisation du premier test technique du PCA non pertinente	Premier test technique de l'ensemble des composantes du PCA (PCA et PRA des métiers et fonctions supports, PSI, PCA global et gestion de crise) organisé,	Défaillance du dispositif ou de l'une de ses composantes non détecté en amont de la survenance d'une crise Dommage subis plus importants, vulnérabilité accrue de l'organisation aux sinistres	Réalisation d'un premier test technique du PCA dans le cadre de son déploiement et portant sur l'ensemble de ses composantes	Vérifier qu'un premier test technique du PCA est prévu et réalisé Revue du programme du premier test technique du PCA, et vérifier qu'il en inclut bien toutes les composantes Audit post test pour en évaluer la qualité

			Absence ou mauvaise préparation et communication préalable au premier test technique du PCA	réalisé et documenté			
	Test des PCA et PRA des métiers et fonctions supports	S'assurer qu'un test de chaque PCA et PRA des métiers et fonctions supports est intégré de manière pertinente dans le premier test technique du PCA	Absence de réalisation d'un test de chaque PCA et PRA des métiers et fonctions supports dans le cadre du premier test technique du PCA Conception et organisation des tests des PCA et PRA métiers et fonctions supports non pertinente Absence ou mauvaise préparation et communication préalable aux tests des PCA et PRA des métiers et fonctions supports Mauvaise articulation des tests des PCA et PRA des métiers et fonctions supports entre eux			Intégration d'un test de chaque PCA et PRA des métiers et fonctions supports des activités critiques dans le premier test technique du PCA	Revue du programme du premier test technique du PCA afin de vérifier qu'il intègre bien tous les PCA et PRA des métiers et fonctions supports de l'organisation Evaluation de la pertinence de la conception, de l'organisation, de la préparation et de la communication des tests des PCA et PRA des métiers et fonctions supports, et notamment leur coordination entre eux (en termes de mobilisation simultanée de ressources) Audit post test pour en évaluer la qualité
	Test du PSI	S'assurer qu'un test du PSI est intégré de manière pertinente dans le premier test technique du PCA Vérifier que le test du PSI prévoit une simulation contrôlée d'indisponibilité du système d'informations de l'organisation	Absence de réalisation d'un test du PSI dans le cadre du premier test technique du PCA Absence de simulation contrôlée d'indisponibilité de l'environnement informatique lors de ce test Simulation d'indisponibilité de l'environnement informatique mal conçue, mal organisée et/ou mal préparée, et donc mal contrôlée Conception et organisation du test du PSI non pertinente Absence ou mauvaise préparation et communication préalable au test du PSI			Intégration du test du PSI dans le premier test technique du PCA, et notamment une simulation contrôlée de l'indisponibilité de l'environnement informatique Vérification du maintien des systèmes et applications critiques	Revue du programme du premier test technique du PCA afin de vérifier qu'il intègre bien le test du PSI de l'organisation Vérification de la prévision d'une simulation contrôlée d'indisponibilité du système d'informations de l'organisation dans le cadre du test du PSI Evaluation de la pertinence de la conception, de l'organisation, de la préparation et de la communication du test du PSI Audit post test pour en évaluer la qualité
	Test du PCA global et de la gestion de crise	S'assurer qu'un test du PCA global et de la gestion de crise est intégré de manière pertinente dans le premier test technique du PCA Vérifier que le test du PCA global et de la gestion de crise prévoit	Absence de réalisation d'un test du PCA global et de gestion de crise dans le cadre du premier test technique du PCA Absence de simulation d'un scénario de crise lors de ce			Intégration du test du PCA global et de la gestion de crise dans le premier test technique du PCA, de manière à contrôler la sécurité et la logistique de crise, les	Revue du programme du premier test technique du PCA afin de vérifier qu'il intègre bien le test du PCA global et de la gestion de crise de l'organisation Vérification de la prévision d'une simulation d'un scénario de crise dans le cadre du test du PCA global et de la

		une simulation d'un scénario de crise	test Simulation de scénario de crise mal conçue, mal organisée et/ou mal préparée, et donc mal contrôlée Conception et organisation du test du PCA global et de la gestion de crise non pertinente Absence ou mauvaise préparation et communication préalable au test du PCA global et de la gestion de crise			dispositifs d'alerte et d'escalade, d'accompagnement du déploiement du PCA puis du PRA, ainsi que pour vérifier la coordination de toutes les composantes du PCA entre elles Simulation d'un scénario de crise afin de mener à bien ce test	gestion de crise Evaluation de la pertinence de la conception, de l'organisation, de la préparation et de la communication du test du PCA global et de la gestion de crise Audit post test pour en évaluer la qualité
	Test des partenaires externes	S'assurer que les partenaires concernés participent au premier test technique du PCA de l'organisation	Absence ou insuffisante sollicitation et mobilisation des partenaires concernés dans le cadre du premier test technique du PCA Mauvaise articulation entre l'organisation et ses partenaires concernés pour le premier test technique du PCA Conception et organisation du premier test technique du PCA avec les partenaires non pertinente Absence ou mauvaise préparation et communication préalable au premier test technique du PCA avec les partenaires	Contractualisation et organisation de la participation des partenaires externes au premier test technique du PCA Documentation de cette participation		Participation des partenaires externes concernés dans le premier test technique du PCA	Revue du programme du premier test technique du PCA afin de vérifier qu'il intègre bien la participation des partenaires de l'organisation concernés Evaluation de la pertinence de la conception, de l'organisation, de la préparation, de la coordination et de la communication du test avec les partenaires Audit post test pour en évaluer la qualité
	Débriefing et retour d'expérience	S'assurer qu'un journal de bord est correctement tenu lors de la réalisation du premier test technique du PCA, qu'il est documenté et conservé dans un souci de traçabilité, et qu'il sert de base au débriefing et au retour d'expérience sur le premier test technique du PCA S'assurer que le retour d'expérience sur le premier test technique du PCA est réalisé, qu'il est utile et permet de constater des dysfonctionnements et axes d'amélioration, et qu'il donne lieu à la mise en place de plans	Absence ou mauvaise tenue d'un journal de bord lors de la réalisation du premier test technique du PCA Absence ou mauvaise documentation et archivage du journal de bord du premier test technique du PCA pour traçabilité Absence ou mauvaise exploitation du journal de bord pour réaliser le débriefing et le retour d'expérience sur le premier test technique du PCA Absence de débriefing et retour d'expérience sur le	Retour d'expérience sur le premier test technique du PCA formalisé	Absence d'amélioration du dispositif	Tenue d'un journal de bord lors de la réalisation du premier test technique du PCA pour assurer la traçabilité et permettre un débriefing et un retour d'expérience sur le test Réalisation d'un débriefing et d'un retour d'expérience pertinent et utile sur le premier test technique du PCA Analyse des résultats du test pour un relevé des dysfonctionnements et	Revue du journal de bord du premier test technique du PCA Revue du mode de documentation et conservation du journal de bord du premier test technique du PCA Revue de la méthode de préparation du débriefing et du retour d'expérience Revue du contenu du retour d'expérience, et vérifier qu'il identifie les dysfonctionnements et axes d'amélioration du PCA Vérifier que les constats du retour d'expérience du premier test technique du PCA donnent lieu à la mise en place de plans d'actions pour amélioration du dispositif de continuité d'activité de l'organisation

		d'actions pour l'amélioration continue du dispositif	premier test technique du PCA Retour d'expérience inutile, sans analyse des résultats pour dégager les dysfonctionnements et axes d'amélioration constatés Absence ou mauvaise mise en place d'un plan d'actions relatif à ces dysfonctionnements et axes d'amélioration pour l'amélioration continue du dispositif de continuité d'activité de l'organisation			axes d'améliorations du PCA constatés pendant le test, et préparation d'un plan d'actions pour l'amélioration continue du dispositif	

3.3.3 La maintenance du PCA

Etapes de mise en place d'un PCA et d'une gestion de crise : Composantes du Contrôle Interne		Finalités : Objectifs de Contrôle Interne Objectifs d'Audit	RISQUES			Bonnes pratiques de Contrôle Interne	Techniques d'audit
			Facteurs (Scénarios d'empêchement)	Points de contrôle	Impacts		
Veille des évolutions contextuelles	Facteurs d'évolution	S'assurer qu'une veille des évolutions normatives et règlementaires relatives au PCA est réalisée, et qu'elle donne lieu à la mise à jour régulière du PCA de l'organisation en conséquence S'assurer que cette veille et ces mises à jour sont traçables	Absence ou insuffisance de la veille des évolutions règlementaires ou normatives Absence ou mauvaise prise en compte de ces évolutions pour mise à jour du PCA de l'organisation Régularité des mises à jour insuffisante ou inadaptée Absence ou mauvaise traçabilité de ces éléments	Veille formalisée des évolutions de la règlementation et des normes	Méconnaissance des évolutions susceptibles d'affecter le dispositif de continuité d'activité Absence de mise à jour du dispositif de continuité d'activité, alors que cela serait nécessaire à la suite des évolutions de l'environnement PCA inopérant, avec des acteurs non informés et formés, inadapté aux besoins de l'organisation ou non conforme aux règlementations, normes et exigences de la Direction Générale et des parties prenantes	Veille des évolutions normatives et règlementaires relatives au PCA pour mise à jour de celui-ci Traçabilité de la veille réalisée et des mises à jour du PCA	Consulter les éléments de traçabilité de la veille des évolutions normatives et règlementaires réalisée, ainsi que de la mise à jour du PCA qui en découle, afin d'en vérifier l'effective réalisation Contrôler rapidement les éléments du PCA de l'organisation liés à des évolutions normatives et règlementaires récentes et vérifier qu'ils ont été mis à jour Evaluer la pertinence de la régularité des mises à jour du PCA au regard de ces éléments
		S'assurer qu'un suivi des évolutions relatives à la stratégie et aux objectifs de l'organisation est réalisé, et qu'il donne lieu à la mise à jour régulière du PCA de l'organisation en conséquence S'assurer que ce suivi et ces mises à jour sont traçables	Absence ou insuffisance du suivi des évolutions relatives à la stratégie et aux objectifs de l'organisation Absence ou mauvaise prise en compte de ces évolutions pour mise à jour du PCA de l'organisation Régularité des mises à jour insuffisante ou inadaptée Absence ou mauvaise traçabilité de ces éléments	Veille formalisée des évolutions de la stratégie de l'organisation		Suivi des évolutions relatives à la stratégie et aux objectifs de l'organisation, afin de mettre à jour la stratégie de continuité et le PCA en conséquence Traçabilité de ce suivi et des mises à jour du PCA	Consulter les éléments de traçabilité du suivi des évolutions relatives à la stratégie et aux objectifs de l'organisation, ainsi que de la mise à jour du PCA qui en découle, afin d'en vérifier l'effective réalisation Contrôler rapidement les éléments du PCA de l'organisation liés à des évolutions de stratégie ou d'objectifs de l'organisation récentes et vérifier qu'ils ont été mis à jour Evaluer la pertinence de la régularité des mises à jour du PCA au regard de ces éléments
		S'assurer qu'un suivi des évolutions du marché sur lequel évolution l'organisation, de sa position sur ce marché et notamment des parts de marché qu'elle détient est réalisé, et qu'il donne lieu à la mise à jour régulière du PCA de l'organisation en conséquence S'assurer que ce suivi et ces mises à jour sont traçables	Absence ou insuffisance du suivi des évolutions du marché sur lequel évolue l'organisation, de sa position sur ce marché et notamment des parts de marché qu'elle détient Absence ou mauvaise prise en compte de ces évolutions pour mise à jour du PCA de l'organisation Régularité des mises à jour insuffisante ou inadaptée Absence ou mauvaise traçabilité de ces éléments	Veille formalisée des évolutions du marché		Suivi des évolutions du marché sur lequel évolue l'organisation, ainsi que de la position de l'organisation sur ce marché, et ses parts de marché notamment, afin de mettre à jour la stratégie de continuité et le PCA en conséquence Traçabilité de ce suivi et des mises à jour du PCA	Consulter les éléments de traçabilité du suivi des évolutions du marché sur lequel évolue l'organisation, de sa position sur ce marché et notamment des parts de marché qu'elle détient, ainsi que de la mise à jour du PCA qui en découle, afin d'en vérifier l'effective réalisation Contrôler rapidement les éléments du PCA de l'organisation susceptibles d'être impactés par ce type d'évolutions et vérifier qu'ils ont été mis à jour Evaluer la pertinence de la régularité des mises à jour du PCA au regard de ces éléments

		S'assurer qu'un suivi des évolutions liées aux partenaires externes de l'organisation, en particulier celles concernant des exigences des parties prenantes envers l'organisation et l'évolution des partenariats est réalisé, et qu'il donne lieu à la mise à jour régulière du PCA de l'organisation en conséquence S'assurer que ce suivi et ces mises à jour sont traçables	Absence ou insuffisance du suivi des évolutions liées aux partenaires externes de l'organisation, en particulier celles concernant les exigences des parties prenantes envers l'organisation et l'évolution des partenariats Absence ou mauvaise prise en compte de ces évolutions pour mise à jour du PCA de l'organisation Régularité des mises à jour insuffisante ou inadaptée Absence ou mauvaise traçabilité des éléments	Veille formalisée des évolutions des partenaires externes		Suivi des évolutions liées aux partenaires externes de l'organisation, en particulier celles concernant les exigences des parties prenantes envers l'organisation et l'évolution des partenariats, afin de mettre à jour la stratégie de continuité et le PCA en conséquence Traçabilité de ce suivi et des mises à jour du PCA	Consulter les éléments de traçabilité du suivi des évolutions liées aux partenaires externes de l'organisation, en particulier celles concernant les exigences des parties prenantes envers l'organisation et l'évolution des partenariats, ainsi que de la mise à jour du PCA qui en découle, afin d'en vérifier l'effective réalisation Contrôler rapidement les éléments du PCA de l'organisation susceptibles d'être impactés par ce type d'évolutions et vérifier qu'ils ont été mis à jour Evaluer la pertinence de la régularité des mises à jour du PCA au regard de ces éléments
		S'assurer qu'un suivi des évolutions liées au personnel de l'organisation, en particulier les entrées, sorties, mutations, promotions et formations des collaborateurs est réalisé, et qu'il donne lieu à la mise à jour régulière du PCA de l'organisation en conséquence, notamment les acteurs identifiés, ainsi que les rôles, responsabilités, pouvoirs et délégations de ces acteurs S'assurer que ce suivi et ces mises à jour sont traçables	Absence ou insuffisance du suivi des évolutions liées au personnel de l'organisation, en particulier les entrées, sorties, mutations, promotions et formations des collaborateurs Absence ou mauvaise prise en compte de ces évolutions pour mise à jour du PCA de l'organisation, et notamment les acteurs identifiés, ainsi que les rôles, responsabilités, pouvoirs et délégations de ces acteurs Régularité des mises à jour insuffisante ou inadaptée Absence ou mauvaise traçabilité des éléments	Veille formalisée des changements de personnel		Suivi des évolutions liées au personnel de l'organisation, en particulier les entrées, sorties, mutations, promotions et formations des collaborateurs, afin de mettre à jour le PCA en conséquence, et notamment les acteurs identifiés, ainsi que les rôles, responsabilités, pouvoirs et délégations de ces acteurs Traçabilité de ce suivi et des mises à jour du PCA	Consulter les éléments de traçabilité du suivi des évolutions liées au personnel de l'organisation ainsi que la mise à jour du PCA qui en découle, notamment les acteurs identifiés, notamment les rôles, responsabilités, pouvoirs et délégations de ces acteurs, afin d'en vérifier l'effective réalisation Contrôler rapidement les acteurs identifiés, ainsi que leurs rôles, responsabilités, pouvoirs et délégations et les rapprocher des évolutions récentes du personnel pour vérifier qu'ils ont été mis à jour Evaluer la pertinence de la régularité des mises à jour du PCA au regard de ces éléments
	Mise à jour des cartographies des processus et des risques	S'assurer que les cartographies des risques et des processus sont régulièrement mises à jour à la suite des évolutions contextuelles et stratégiques, et que ces mises à jour sont traçables	Mauvaise ou incomplétude de l'élaboration des cartographies des processus et des risques (Cf. Conception du PCA) Absence, insuffisance ou mauvaise mise à jour des cartographies des processus et des risques Absence ou mauvaise prise en compte des évolutions contextuelles et stratégiques pour la mise à jour des cartographies des processus et des risques	Mise à jour des cartographies des processus et des risques (numéros de versions)	Dispositif de continuité d'activité non maintenu en condition opérationnelle PCA inopérant et/ou non conforme	Mise à jour des cartographies des processus et des risques à la suite des évolutions contextuelles et stratégiques Traçabilité de la mise à jour des cartographies des risques et des processus	Consulter les éléments de traçabilité de la mise à jour des cartographies des processus et des risques, afin d'en vérifier l'effective réalisation Contrôler les cartographies des processus et des risques et en évaluer la qualité et la complétude Contrôler en particulier les éléments des cartographies des processus et des risques susceptibles d'être impactés par les évolutions contextuelles et stratégiques récentes et vérifier qu'ils ont été mis à jour Evaluer la pertinence de la régularité des mises à jour des cartographies des

			Régularité des mises à jour insuffisante ou inadaptée Absence ou mauvaise traçabilité des mises à jour				processus et des risques au regard de ces éléments
	Mise à jour des analyses d'impact et de la stratégie de continuité	S'assurer que les analyses d'impact et la stratégie de continuité sont régulièrement mises à jour à la suite des évolutions des cartographies des processus et des risques, et que ces mises à jour sont traçables	Mauvaise élaboration des analyses d'impact et de la stratégie de continuité (Cf. Conception du PCA) Absence, insuffisance ou mauvaise mise à jour des analyses d'impact et de la stratégie de continuité Absence ou mauvaise prise en compte des évolutions des cartographies des processus et des risques pour la mise à jour des analyses d'impact et de la stratégie de continuité Régularité des mises à jour insuffisante ou inadaptée Absence ou mauvaise traçabilité des mises à jour	Mise à jour des analyses d'impact et de la stratégie de continuité (numéros de versions)		Mise à jour des analyses d'impact et de la stratégie de continuité à la suite des évolutions des cartographies des processus et des risques Traçabilité de la mise à jour des analyses d'impact et de la stratégie de continuité	Consulter les éléments de traçabilité de la mise à jour des analyses d'impact et de la stratégie de continuité, afin d'en vérifier l'effective réalisation Contrôler les analyses d'impact et la stratégie de continuité et en évaluer la qualité Contrôler en particulier les éléments des analyses d'impact et de la stratégie de continuité susceptibles d'être impactés par les évolutions récentes des cartographies des processus et des risques et vérifier qu'ils ont été mis à jour Evaluer la pertinence de la régularité des mises à jour des analyses d'impact et de la stratégie de continuité au regard de ces éléments
Tests réguliers du PCA	S'assurer que des tests réguliers du PCA sont réalisés dans le cadre de son maintien en condition opérationnelle, et qu'ils sont faits conformément aux bonnes pratiques déployés dans le cadre du premier test technique du PCA (Cf. Déploiement du PCA)	Absence ou mauvaise sensibilisation des acteurs et de la gouvernance à la nécessité de réaliser des tests réguliers du PCA afin de le maintenir en condition opérationnelle Absence ou insuffisance de la planification et la réalisation de tests réguliers Tests réguliers du PCA non conformes aux bonnes pratiques déployées dans le cadre du premier test technique du PCA (Cf. Déploiement du PCA)	Tests réguliers de l'ensemble des composantes du PCA organisés, réalisés et documentés Contractualisation et organisation de la participation des partenaires externes aux tests Retour d'expérience sur les tests du PCA formalisés	Méconnaissance des défaillances de tout ou partie du PCA (suite aux évolutions survenues depuis le déploiement initial) Absence d'exercice pratique pour le nouveau personnel arrivé après le déploiement initial (formation incomplète) Absence de retour d'expérience sur les tests donc absence d'amélioration continue du dispositif	Réalisation de tests réguliers du PCA dans le cadre de son maintien en condition opérationnelle Conformité de ces tests réguliers avec les bonnes pratiques déployées dans le cadre du premier test technique du PCA (Cf. Déploiement du PCA)	Consulter le programme de maintien en condition opérationnelle et le programme de test pour vérifier que des tests réguliers sont effectivement programmés Consulter les éléments de traçabilité de la réalisation de ces tests (journaux de bord, retours d'expériences, plans d'actions qui en découlent…) afin de vérifier qu'ils ont effectivement été réalisés Dérouler les mêmes points d'audit que lors de l'audit du premier test technique du PCA pour chacun de ces tests réguliers de maintenance
Mise à jour des évaluations financières	S'assurer que les évaluations financières du PCA sont régulièrement mises à jour en tenant compte de l'ensemble des évolutions impactantes, et que ces mises à jour sont traçables	Chiffrage erroné (Cf. Conception du PCA) Absence ou mauvaise réactualisation des évaluations financières du PCA Absence ou mauvaise prise en compte de l'ensemble des éléments d'évolution pour la	Mise à jour des évaluations financières (numéros de version)	Evaluations financières déconnectées de la réalité Budget et ressources allouées inadaptés Impossibilité de déployer les PCA	Réactualisation régulière du chiffrage des PCA Traçabilité des mises à jour des évaluations financières	Consulter les éléments de traçabilité des mises à jour des évaluations financières du PCA afin d'en vérifier l'effective réalisation Contrôler les évaluations financières et leur méthode d'élaboration et en évaluer la qualité Contrôler en particulier les éléments des évaluations financières

		réactualisation financière Régularité des mises à jour insuffisante ou inadaptée Absence ou mauvaise traçabilité des mises à jour				susceptibles d'être impactés par des évolutions récentes et vérifier qu'ils ont été mis à jour Evaluer la pertinence de la régularité des mises à jour des évaluations financières, notamment au regard de ces éléments
Mise à jour des procédures	S'assurer que l'ensemble des procédures du PCA sont mises à jour régulièrement à la suite des différentes évolutions	Absence ou mauvaise mise à jour des procédures du PCA Non considération de toutes les procédures de toutes les composantes du PCA à mettre à jour Absence ou mauvaise prise en compte des évolutions pour la mise à jour des procédures Régularité des mises à jour insuffisante ou inadaptée Absence ou mauvaise traçabilité des mises à jour	Mise à jour des procédures de continuité d'activité (numéros de version)	Procédures obsolètes et inopérantes Continuité des activités critiques de l'organisation à leur niveau de service minimum non assurée	Mise à jour de l'ensemble des procédures du PCA suite aux évolutions précédemment évoquées Traçabilité des mises à jour des procédures	Consulter les éléments de traçabilité des mises à jour des procédures du PCA afin d'en vérifier l'effective réalisation Vérifier que les mises à jour portent bien de manière exhaustive sur toutes les procédures de toutes les composantes du PCA Contrôler les éléments des procédures susceptibles d'être impacté par des évolutions récentes et vérifier qu'ils ont été mis à jour Evaluer la pertinence de la régularité des mises à jour des procédures du PCA

3.4 Référentiels spécifiques sectoriels

3.4.1 Secteur bancaire

Activités critiques : Composantes du Contrôle Interne	Finalités : Objectifs de Contrôle Interne Objectifs d'Audit	RISQUES			Bonnes pratiques de Contrôle Interne	Techniques d'Audit
		Facteurs (Scénarios d'empêchement)	Points de contrôle	Impacts		
Organisation et pilotage	S'assurer qu'un RPCA et RPSI ont été désignés S'assurer de la bonne définition des fonctions et des responsabilités des acteurs de la continuité d'activité S'assurer de la définition des schémas hiérarchiques entre les acteurs du PCA et de la gestion de crise S'assurer que tous les acteurs du comité de pilotage des PCA participent à la démarche S'assurer que des reporting réguliers aux instances de pilotage sont effectués	Absence d'interlocuteurs identifiés	Acteurs de la démarche identifiés Rôles, responsabilités et pouvoirs formalisés	La non désignation formelle des acteurs du PCA et PSI est vecteur d'un dispositif désorganisé et inefficace	Formalisation des relations hiérarchiques et du schéma délégataire des organes de gouvernance du PCA Désignation des acteurs principaux de la démarche PCA et PSI	Vérification de la bonne formalisation de l'organigramme et des schémas délégataires pour l'organe de pilotage du PCA Revue des comptes-rendus des Comités de Pilotage Vérification de l'existence de reportings ascendants réguliers
Contrôles permanents et conformité règlementaire	S'assurer que des contrôles permanents couvrent le périmètre du PCA et de la gestion de crise, notamment portant sur la conformité aux impératifs règlementaires S'assurer de la présence de ces contrôles dans le plan de contrôle S'assurer de la pertinence des contrôles, de leur bonne exécution et de la clôture des recommandations ainsi que des plans d'actions	Mauvaise définition des contrôles permanents (insuffisant pour couvrir tout le périmètre du PCA et de la gestion de crise, ou ne permettant pas de s'assurer de la conformité règlementaire) Absence ou mauvaise réalisation des contrôles permanents	Plan de contrôle Livrables des contrôles permanents	Absence de couverture des risques critiques Non-conformité aux dispositions légales entourant les PCA Sanctions financières des instances de tutelle	Formalisation de contrôles permanents sur le périmètre du PCA et de la gestion de crise Formalisation de contrôles de conformité au respect des dispositions légales du secteur bancaire	Vérification de la cartographie des risques opérationnels Vérification de la complétude le plan de contrôle de la direction des contrôles permanents et risques Vérification de la clôture des recommandations de l'audit sur le périmètre PCA et de la clôture des plans d'actions émis sur le périmètre PCA
PSI	S'assurer que le PSI soit documenté	Mauvaise définition du PSI	PSI formalisé et	Perte des	Mise en place d'un PSI	Revue de la documentation

	S'assurer de la bonne formalisation et de la validation du comité de pilotage et de la DG, des besoins du PSI S'assurer que la politique de sauvegarde couvre les données et le système S'assurer de la non exposition des systèmes aux risques physiques S'assurer de la formalisation des contrats entre l'entité et les prestataires du PSI S'assurer de l'existence de tests et de mises à jour réguliers du PSI	(mauvaise identification et validation des besoins, solutions de continuité inefficaces ou inefficientes Exposition du matériel aux risques physiques, Absence ou mauvaise contractualisation avec les prestataires Absence de tests et mises à jour réguliers du PSI	documenté Protection du matériel Contractualisation avec les prestataires Rapports des tests et mises à jour du PSI	applicatifs et donnés critiques pour la continuité de l'organisation : Impossibilité de déployer les dispositifs de continuité	pertinent et documenté Validation du Plan de Secours Informatique par le comité de pilotage Définition et pertinence des besoins relatifs à la mise en place du PSI Sécurisation de la sauvegarde des systèmes et données critiques	autour des PSI Revue des contrats de prestation de service pour les PSI Inventaire des sites de repli et évaluation de la pertinence de leur situation géographique et de leur équipement par rapport au site de production et aux besoins en continuité informatique Revue des tests du PSI effectués dans l'année
Plan de repli utilisateurs	S'assurer de l'existence d'un plan de repli utilisateur S'assurer de la présence des équipements nécessaires à la continuité, notamment informatique, de l'activité sur les sites de repli utilisateurs S'assurer de la bonne transférabilité des données et applicatifs sensibles aux sites de secours S'assurer que les contrats avec les prestataires pour les sites de repli soient correctement formalisés S'assurer de l'existence de tests de repli utilisateurs réguliers	Absence de plan de repli utilisateur	Plan de repli formalisé Contractualisation avec les prestataires Rapports des tests du plan de repli	Impossibilité de déployer les dispositifs de continuité due à l'absence ou à l'inaccessibilité du matériel et des moyens nécessaires (notamment informatiques)	Formalisation des contrats de prestations de services : prévision d'un site de repli utilisateurs Transférabilité des applicatifs et des bases de données sur les sites de repli	Revue des contrats avec les fournisseurs de site de repli Revue des modalités de contrat avec les prestataires Evaluation des modalités de transfert des données informatiques Revue et évaluation des équipements des sites de repli
PSEE	S'assurer de la bonne formalisation des contrats avec les prestataires de services essentiels (dans le cadre des PCA) et de leur conformité aux dispositions règlementaires	Absence de formalisation des contrats	Contractualisation avec les prestataires	Non-respect des dispositions légales Sanctions des instances de tutelle	Formalisation et conformité des contrats de prestation de services essentiels externalisés	Revue des contrats de prestation de services Vérification de la conformité des accords PSEE avec les dispositions du CRBF 97-02

3.4.2 Secteur de la santé publique

Activités critiques : Composantes du Contrôle Interne	Finalités : Objectifs de Contrôle Interne Objectifs d'Audit	RISQUES			Bonnes Pratiques de Contrôle Interne	Techniques d'Audit
		Facteurs (Scénarios d'empêchement)	Points de contrôle	Impacts		
Fonctionnement du matériel biomédical	S'assurer qu'une procédure dégradée de continuité en cas de défaillance d'un dispositif médical est formalisée S'assurer que le personnel est informé et formé sur cette procédure	Procédure non formalisée Personnel non informé ou non formé	Procédure de continuité de fonctionnement du matériel biomédical Formations dispensées au personnel biomédical	Report d'interventions, de rendez-vous Problèmes graves, voire décès des patients	Dispositif de continuité en cas de défaillance d'un dispositif médical (en mode dégradé)	Revue de la procédure dégradée de continuité en cas de défaillance d'un dispositif médical Consulter le listing des formations annuelles, et le rapprocher du personnel en poste
Services techniques (alimentation en énergie et fluides)	S'assurer que des dispositifs pertinents de continuité d'alimentation en énergie et en fluides sont prévus et leurs modes d'activation et de fonctionnement formalisés	Absence de dispositif de continuité d'alimentation en énergie Absence de dispositif de continuité d'alimentation en fluides	Dispositifs formalisés de continuité d'alimentation en énergies et fluides	Interruption de fonctionnement du matériel et des infrastructures Impossibilité de déployer les dispositifs de continuité qui reposent sur ces moyens	Dispositif de continuité d'alimentation en énergie (groupes électrogènes, redondance des alimentations…) Dispositif de continuité d'alimentation en fluides (eau, oxygène…) comme des réservoirs de secours ou une redondance des alimentations	Revue des dispositifs de continuité d'alimentation en énergie et en fluides afin de s'assurer de leur existence et de leur pertinence (valider leur efficacité et leur efficience théorique) Test effectif des dispositifs via une interruption contrôlée de l'alimentation en énergie et en fluides
Approvisionnements	S'assurer qu'un dispositif de continuité d'activité pertinent est prévu en cas d'interruption des approvisionnements clés, qu'il est formalisé et que le personnel concerné est formé	Absence de stock de sécurité défini et/ou maintenu Stock de sécurité non optimal Absence de mode d'approvisionnement alternatif prévu et contractualisé	Stock de sécurité Mode d'approvisionnement alternatif Contractualisation avec les fournisseurs	Reports d'intervention Préjudices pour les patients	Dispositif de continuité d'activité en cas d'interruption des approvisionnements clés (médicaments critiques, sang, matériel de première nécessité…) tel qu'un stock de sécurité ou un mode d'approvisionnement	Vérification de la définition et du maintien d'un stock de sécurité pour les approvisionnements critiques Revue des modes d'approvisionnements alternatifs et de leur correcte contractualisation

					alternatif	
Gestion de crise : Plans blancs interne	S'assurer qu'un plan blanc interne pertinent est correctement formalisé, qu'il répond aux exigences règlementaires, et qu'il fait l'objet d'une bonne allocation des ressources et d'une bonne formation du personnel	Absence ou mauvaise formalisation d'un dispositif de plan blanc interne Non pertinence du dispositif Mauvaise allocation des ressources et moyens au plan blanc interne, absence ou mauvaise formation du personnel	Plan blanc interne formalisé et documenté	Sanctions envers l'établissement Incapacité de l'établissement à répondre à un afflux massif de victimes Dégâts humains Dégradation de l'image de l'établissement	Formalisation d'un dispositif de plan blanc interne conforme aux exigences règlementaires	Revue du dispositif de plan blanc interne, des rôles et responsabilités des acteurs et des ressources allouées Consulter le listing des formations dispensées autour du plan blanc interne et le rapprocher du personnel en poste Test effectif des dispositifs via une simulation
Gestion de crise : Insertion dans les dispositifs globaux (plan blanc élargi, plans d'urgence)	S'assurer qu'un dispositif pertinent d'intégration dans les dispositifs globaux est correctement formalisé, qu'il répond aux exigences règlementaires, et qu'il fait l'objet d'une bonne allocation des ressources et d'une bonne formation du personnel	Absence ou mauvaise formalisation du dispositif d'intégration dans les plans globaux Non pertinence du dispositif Mauvaise allocation des ressources et moyens au dispositif, absence ou mauvaise formation du personnel	Dispositif d'intégration dans les dispositifs d'urgence globaux		Dispositif formalisé d'intégration de l'établissement de santé dans les dispositifs globaux	Revue du dispositif d'intégration dans les dispositifs globaux, des rôles et responsabilités des acteurs et des ressources allouées Consulter le listing des formations dispensées sur ce dispositif et le rapprocher du personnel en poste Test effectif des dispositifs via une simulation
SIH (Système d'Information Hospitalier)	S'assurer que les données confidentielles sont sécurisées S'assurer que le dossier patient, les applications critiques et le réseau sont continuellement accessibles	Absence ou mauvais système de sécurisation des données et des accès informatiques Absence ou mauvaise conception et formalisation des dispositifs de continuité d'accès au dossier patient et de fonctionnement des applications critiques et du réseau	PSI formalisé et documenté	Mauvaise protection des données confidentielles Indisponibilité du dossier patient, des applications critiques et du réseau (erreurs médicales, reports d'intervention	Sécurisation des données confidentielles Dispositif de continuité d'accès au dossier patient Continuité de fonctionnement des applications critiques et du réseau (redondances des systèmes, prestataires de secours contractualisés)	Revue du dispositif de sécurisation des données Revue des habilitations et accès informatiques en les rapprochant du personnel actuellement en poste Test d'intrusion dans les bases de données Revue des dispositifs de continuité d'accès au dossier patient et de fonctionnement des applications critiques et du réseau

3.4.3 Secteur alimentaire

Activités critiques : Composantes du Contrôle Interne	Finalités : Objectifs de Contrôle Interne Objectifs d'Audit	RISQUES			Bonnes Pratiques de Contrôle Interne	Techniques d'Audit
		Facteurs (Scénarios d'empêchement)	Points de contrôle	Impacts		
Sécurité des infrastructures et sites de production	S'assurer qu'un site de repli existe, qu'il est suffisamment équipé et opérationnel rapidement S'assurer en cas d'absence de site de repli qu'un autre site peut être opérationnel pour prendre le relais de la production	Absence de site de repli Site de repli non opérationnel rapidement Insuffisance de l'équipement prévu sur le site de repli Site de repli exagérément coûteux Site annexe non équipé pour accueillir du personnel supplémentaire	Site de repli existant	Interruption de la production Impossibilité de déployer les dispositifs de continuité d'activité due à l'absence ou à l'indisponibilité du matériel nécessaire	Continuité des infrastructures de secours ou site de repli Sites de production annexes le cas échéant, équipés pour accueillir le personnel supplémentaire et permettre la continuité	Vérification de l'existence d'un site de repli Revue de l'équipement du site de repli (suffisance, adéquation avec les besoins en continuité, qualité et maintenance) Evaluation de la pertinence des ressources et moyens déployés pour le site de repli Test effectif du site de repli via une simulation de sinistre Test des sites de remplacements
Equipements lourds de production	S'assurer que toutes les mesures de sécurité sont prises lors de l'utilisation des équipements S'assurer que les prestataires de maintenance internes ou externes sont identifiés S'assurer qu'il existe des équipements de secours opérationnels	Mesures de sécurité et consignes d'utilisation du matériel de production non formalisées, non conformes à la règlementation ou non respectées Mauvaise configuration du matériel (température…) Absence de contractualisation de maintenance Absence d'équipements de secours	Mesures de sécurité et consignes d'utilisation du matériel de production formalisées Configuration du matériel Contractualisation avec les prestataires de maintenance Equipements de secours opérationnels et documentés	Incendies Pannes Rupture de la chaîne du froid	Continuité et sécurité des équipements lourds servant à la production et au conditionnement Formalisation de mesures de sécurité et consignes d'utilisation du matériel Contrats de maintenance Equipements de secours opérationnels	Vérification de la viabilité des équipements Revue des contrats de garantie/maintenance Inventaires des équipements existants et équipements de secours Contrôle de la conformité des équipements et de leur utilisation au regard des normes et règles sanitaires
Chaine de production	S'assurer que les relations	Absence de contractualisation de la	Contractualisation de la continuité d'activité	Défaillance de la continuité d'activité	Chaine de production depuis la livraison de la	Revue de contrats de prestations de services externalisés

	d'interdépendance entre les fournisseurs sont identifiées et formalisées S'assurer de la capacité de l'entreprise à continuer la production dans le cas où un évènement viendrait handicaper une étape essentielle dans le processus de fabrication	continuité d'activité avec les partenaires et fournisseurs Absence de dispositifs palliatifs de continuité d'activité en cas de défaillance des fournisseurs et partenaires	avec les fournisseurs et partenaires Dispositifs palliatifs de continuité d'activité en cas de défaillance des fournisseurs et partenaires	des fournisseurs et partenaires : Rupture de la chaîne de production Impossibilité de déployer les dispositifs de continuité du fait de la défaillance des partenaires	matière première, jusqu'au conditionnement et à la distribution Relations d'interdépendances entre les sites de production avec les fournisseurs, prestataires de services externalisés ou partenaires	Revue des contrats avec les partenaires et de leurs modalités
Sécurité alimentaire	S'assurer que toutes les règles et normes de sécurité alimentaires en vigueur sont respectées S'assurer du bon conditionnement des aliments et de leur transport en toute sécurité (non rupture de la chaine du froid, protection des aliments, etc.)	Non-respect des normes d'hygiène (Contamination des aliments par le personnel) Incident dans les entrepôts Mauvais fonctionnement des infrastructures Actes de malveillance : Contamination de produits Conditionnement des aliments non conforme	Normes d'hygiène formalisées Conditionnements des aliments Contrôle et maintenance du matériel	Dégâts Humains Dégradation de l'image de l'organisation Conséquences financières (retrait du marché d'un très grand nombre de produits en cas de problème)	Dispositif efficace et fiable de garantie de la viabilité des denrées alimentaires tout au long de la chaine de production de façon à préserver la sécurité des consommateurs	Contrôle de la conformité aux règles sanitaires Contrôle des conditionnements des aliments Contrôle du respect de la chaine du froid
Alimentation en énergie	S'assurer que des dispositifs pertinents sont prévus et opérants pour garantir la continuité d'alimentation en énergie	Absence ou non pertinence du ou des dispositifs de continuité de l'alimentation en énergie Dysfonctionnements des dispositifs de secours (mauvaise qualité ou mauvais entretien du matériel) Mauvaise contractualisation du recours à des prestataires de secours	Dispositifs de continuité d'alimentation en énergie	Interruption de la production Impossibilité de déployer les dispositifs de continuité qui nécessitent une alimentation en énergie	Dispositif efficace, pertinent et fiable de continuité de l'alimentation en énergie, tels que la redondance des systèmes d'alimentations, des groupes électrogènes ou des prestataires de secours	Revue des dispositifs de continuité de l'alimentation en énergie et en tester l'efficacité et la pertinence théoriques Vérifier l'obsolescence, la qualité et l'entretien du matériel dédié Vérifier que les dispositifs sont testés régulièrement Tester effectivement les dispositifs de continuité de l'alimentation en énergie via une interruption contrôlée de l'alimentation

3.4.4 Secteur de l'énergie

Activités critiques : Composantes du Contrôle Interne	Finalités : Objectifs de Contrôle Interne Objectifs d'Audit	RISQUES			Bonnes Pratiques de Contrôle Interne	Techniques d'Audit
		Facteurs (Scénarios d'Empêchement)	Points de contrôle	Impacts		
Sécurité du réseau de distribution / transport du gaz et des installations	S'assurer que les réseaux de distribution sont sécurisés et protégés contre d'éventuelles intrusions S'assurer des contrôles réguliers des réseaux de transports du gaz S'assurer que les installations sont toujours d'actualité	Absence ou mauvaise sécurisation des réseaux de distribution et de transport du gaz Absence de contrôles réguliers, maintenance et réfections des réseaux	Dispositifs de sécurisation des réseaux Rapports de contrôles, maintenance et réfection des réseaux	Accidents (explosions) Dégâts humains	Formalisation et mise en place de dispositifs de sécurisation des réseaux Contrôles, maintenance et réfections réguliers des réseaux	Appréciation et contrôle de la sécurité des réseaux de transport et de distribution du gaz Contrôle du fonctionnement des systèmes d'alarmes Revue des remontées d'incidents Evaluer l'obsolescence des installations Revue des réhabilitations
Approvisionnement en gaz	S'assurer que les stocks disponibles permettent la continuité d'activité en cas de d'approvisionnements dus à des baisses d'exportations de la part des pays fournisseurs (Russie, Maghreb)	Arrêt partiel ou total de l'approvisionnement en gaz des pays fournisseurs Absence de dispositifs palliatifs pour assurer la continuité des approvisionnements	Accords avec les fournisseurs principaux Stocks disponibles Dispositifs palliatifs d'approvisionnement	Pénurie	Dispositifs palliatifs en cas d'interruption d'approvisionnement : Stocks de sécurité, contrats d'approvisionnements avec des fournisseurs alternatifs	Contrôle des niveaux des stocks Revue des accords d'importation Multiplicité des pays partenaires
Espaces de stockage du gaz	S'assurer que les espaces de stockage du gaz sont hautement sécurisés S'assurer que l'accès à ces sites est règlementé	Absence ou mauvaise sécurisation des lieux de stockage du gaz Absence de contrôles réguliers, maintenance et réfection des lieux de stockage	Dispositifs de sécurisation des lieux de stockage Rapports de contrôles, maintenance et réfection des lieux de stockage	Accidents (explosions) Dégâts humains	Formalisation et mise en place de dispositifs de sécurisation des lieux de stockage Contrôles, maintenance et réfections réguliers des lieux de stockage	Revue des dispositifs de sécurisation des lieux de stockage Contrôle de la viabilité des systèmes anti-intrusion Evaluer l'obsolescence des installations Revue des réhabilitations
Sécurité du personnel et des consommateurs	S'assurer que le dispositif d'urgence sécurité gaz fonctionne correctement et	Vétusté des installations dangereuse pour les consommateurs	Mesures de sécurité formalisées Dispositif d'urgence	Accidents (explosions, asphyxies…)	Protection du personnel et des consommateurs en	Revue de la pertinence des différentes dispositions de sécurité

	que les alertes sont remontées de façon efficaces et donnent lieu à des interventions rapides S'assurer que toutes les mesures de sécurités sont respectées lors des interventions de façon à assurer la protection des consommateurs et du personnel	Absence d'un dispositif d'urgence sécurité gaz Non-respect des mesures de sécurité	sécurité gaz Etat des installations	Dégâts humains	toutes circonstances	Revue des rapports d'intervention du dispositif d'urgence sécurité gaz
Ressources Humaines	S'assurer du recrutement de personnes de compétentes pour garantir la mise en sécurité installations ou des personnes et le diagnostic des incidents S'assurer que les experts de la maintenance des réseaux sont disponibles à tout moment dans l'entité S'assurer de l'existence de « profils clés » dont l'absence paralyserait l'intervention sur les réseaux	Profils inadaptés Personnel indisponible en cas de besoin	Personnel en poste (fiches de postes) Planning et astreintes	Mauvaise gestions des problèmes de terrains Accidents causés par le personnel Absence de profils clés laissant dans l'incapacité de gérer la crise	Procédure de recrutement efficace et adaptée aux besoins opérationnels, de sécurité et en continuité d'activité	Revue des procédures de recrutement et des niveaux de diplômes exigées Evaluation du schéma délégataire Revue du planning et des astreintes
SI Industriels	S'assurer que les postes de supervision et de remontée d'alerte sont viables S'assurer que chaque alerte donc lieu à une intervention S'assurer de leur maintenance	SI inadaptés ou inefficaces Absence ou mauvaise maintenance des SI Absence de dispositif de continuité de fonctionnement des SI industriels	SI industriels Contrats de maintenance Dispositif de continuité de fonctionnement des SI industriels	Absence de visibilité sur le réseau (état, fuites, intrusions…) Accidents (dégâts matériels et humains)	Dispositif de continuité des Si efficace et pertinent Contrats de maintenance des SI industriels	Revue des contrats de maintenance Revue des alertes et de leur résolution (rapports d'intervention)

3.4.5 Secteur des transports

Activités critiques : Composantes du Contrôle Interne	Finalités : Objectifs de Contrôle Interne Objectifs d'Audit	RISQUES			Bonnes Pratiques de Contrôle Interne	Techniques d'Audit
		Facteurs (Scénarios d'empêchement)	Points de contrôle	Impacts		
Sûreté et sécurité des voyageurs (Terrorisme, incendies…)	S'assurer que l'organisation a prévu des dispositifs pour assurer la sécurité des personnes efficaces et pertinents S'assurer que les dispositifs en place sont conformes aux exigences règlementaires	Perte des services de télécommunications externes Indisponibilité des infrastructures et du matériel Indisponibilité du personnel	Dispositifs de sécurité des personnes et garantie de leur continuité de fonctionnement	Dégâts humains Conséquences juridiques, financières (amendes, indemnisations…), et d'image Indisponibilité du personnel	Garantie de la sûreté et de la sécurité des personnes (usagers, voyageurs) en toutes circonstances, en particulier lors de la survenance d'une crise	Revue des dispositifs en les rapprochant des exigences règlementaires Test de cheminement sur le déploiement de ces dispositifs Test effectif des dispositifs via une simulation
Services techniques (alimentation en énergie et fluides)	S'assurer que l'organisation a prévu un système d'alimentation en énergie et en fluides alternatif	Indisponibilité des infrastructures et/ou du personnel	Dispositif d'alimentation en énergie et fluides alternatif	Impossibilité de déployer les dispositifs de continuité qui nécessitent des ressources en énergie et fluides	Mise en place d'un système d'alimentation en énergie et en fluides alternatif (redondance des systèmes d'alimentations, groupes électrogènes, réservoirs d'eau et de combustibles, prestataires de secours…)	Revue des dispositifs Test des dispositifs via une interruption contrôlée de l'alimentation en énergie et fluides
Information aux voyageurs	S'assurer que l'organisation a prévu des dispositifs pour assurer la continuité de l'information aux voyageurs efficaces et pertinents	Perte des services de télécommunications externes ou de l'alimentation en énergie Indisponibilité des infrastructures et du matériel ou du personnel	Dispositif de continuité de l'information aux voyageurs	Sanctions juridiques Insatisfaction des voyageurs (risque d'image)	Diffusion d'informations sur le service assuré et la situation de crise Personnel déployé sur le terrain Système d'affichage papier	Revue des dispositifs Test des dispositifs via une simulation de survenance d'un sinistre
Viabilité hivernale	S'assurer que l'organisation a prévu des dispositifs efficaces et pertinents pour assurer la	Indisponibilité des infrastructures et du matériel	Dispositifs de viabilité hivernale	Sanctions (non-respect des engagements) Pertes financières (baisse	Renforcement des infrastructures Dispositifs spécifiques	Revue des dispositifs en les rapprochant des exigences règlementaires

	continuité d'activité en cas d'intempéries hivernales importantes	Interruption des approvisionnements Indisponibilité du personnel		d'activité) Dégradation de l'image de l'organisation	(baies de dégivrage) Ressources humaines (astreintes) Stocks de produits (sel, dégivrant, déverglaçant)	Test des dispositifs via une simulation d'intempéries
Gestion de crise : Veille permanente	S'assurer que l'organisation a prévu une cellule de veille chargée de collecter les informations adéquates et de suivre les indicateurs pertinents pour détecter en anticiper la survenance d'un sinistre	Absence de cellule de veille Absence ou mauvaise définition des rôles et responsabilités de la cellule de veille Absence ou mauvaise définition des informations et indicateurs à surveiller	Cellule de veille (membres, rôles et responsabilités formalisés) Sélection et suivi des indicateurs Dispositif de veille	Absence de détection des incidents Absence de traitement des incidents mineurs qui deviennent ainsi systématiquement des sinistres de grande ampleur Réaction lente ou inadaptée de l'organisation à un sinistre Dommages subis plus importants Vulnérabilité accrue de l'organisation aux sinistres Sanctions (non-respect des obligations de notification et de retour d'expérience) Absence d'amélioration du dispositif via un retour d'expérience	Collecte des incidents rapportés par d'autres exploitants, la surveillance DGAC, et le personnel Obtention des informations contextuelles (météorologiques…) Suivi des indicateurs d'activité Circulation de l'information en interne	Revue des fonctions, rôles, responsabilités et pouvoirs de la cellule de veille et de ses membres Test d'observation sur la surveillance réalisée Consultation des reportings de la veille réalisée
Gestion de crise : Notification des incidents aux représentants de l'Etat ou au BEA (Bureau d'Enquête et d'Analyse)	S'assurer qu'une procédure de notification est formalisée S'assurer que le personnel responsable est identifié et formé S'assurer que les outils nécessaires à la notification sont disponibles	Absence de procédure de notification formalisée Personnel responsable non identifié et/ou non formé Indisponibilité des outils nécessaires	Procédure de notification Personnel responsable de la notification Outils disponibles et continuité de fonctionnement		Procédure de notification formalisée Personnel identifié et formé Outils disponibles (formulaires)	Revue de la procédure de notification des incidents Consultation de la liste du personnel responsable de la notification et des formations qu'il a reçu sur le sujet
Gestion de crise : Analyse sommaire de l'incident préalablement au déploiement des dispositifs de secours	S'assurer que l'organisation a prévu une analyse sommaire de l'incident préalablement au déploiement des dispositifs, et que le déploiement se base sur cette analyse	Absence ou mauvaise formalisation du mode opératoire de l'analyse Mode opératoire non pertinent Absence ou mauvaise communication interne de l'analyse aux responsables du déploiement des dispositifs	Mode opératoire d'analyse sommaire des incidents		Analyse sommaire de l'incident pour un déploiement des dispositifs pertinent	Revue du mode opératoire d'analyse Test de cheminement sur la communication interne de l'analyse Test sur les incidents passés : Vérifier que l'analyse avait été menée et correctement communiquée, et que le

						déploiement des dispositifs avait été réalisé en conséquence
Gestion de crise : Retour d'expérience	S'assurer que l'organisation a prévu un mode opératoire de retour d'expérience pertinent	Absence ou mauvaise sensibilisation du personnel aux retours d'expérience Absence ou mauvaise formalisation du mode opératoire de retour d'expérience (analyse approfondie de la crise, communication et amélioration des dispositifs) Mode opératoire non pertinent	Mode opératoire de retour d'expérience sur les crises		Analyse approfondie des incidents pour retour d'expérience (à transmettre à l'autorité compétente) Mesures d'amélioration des dispositifs	Revue du mode opératoire de retour d'expérience Test sur les incidents passés : Revue des retours d'expérience réalisés
Spécificités de l'aviation civile : Péril animalier	S'assurer que l'organisation a prévu des dispositifs préventifs, de détection et ponctuels de lutte contre le péril animalier S'assurer que l'organisation dispose de toutes les autorisations nécessaires au déploiement des dispositifs	Absence ou inadéquation des mesures préventives Absence ou mauvaise détection des animaux Non détention des autorisations nécessaires aux mesures ponctuelles (permis de chasse…)	Dispositifs de lutte contre le péril animalier	Explosion d'un réacteur causée par un oiseau Dégâts humains, financiers, juridiques et d'image	Actions préventives visant à rendre le milieu inhospitalier Détection des animaux Mesures ponctuelles d'effarouchement ou de prélèvement d'animaux	Revue des dispositifs prévus eu égard au péril animalier Vérifier les autorisations demandées et obtenues
Spécificités de l'aviation civile : Aide à la navigation (radio et balisage)	S'assurer que les dispositifs prévus permettent de répondre aux exigences règlementaires (de DMIA notamment)	Indisponibilité des infrastructures et du matériel ou du personnel Perte des services de télécommunications externes ou de l'alimentation en énergie	Dispositifs d'aide à la navigation et garantie de leur continuité de fonctionnement	Accidents d'aéronefs Dégâts humains, financiers, juridiques et d'image	Maintien en permanence d'un balisage lumineux des pistes et aires aéronautiques et d'une assistance radio à la navigation	Revue des dispositifs prévus en les rapprochant du référentiel des bonnes pratiques Test des dispositifs via une simulation de sinistre (coupure d'alimentation en énergie, brouillage des télécommunications externes…)

3.4.6 Secteur des télécommunications

Activités critiques : Composantes du Contrôle Interne	Finalités : Objectifs de Contrôle Interne Objectifs d'Audit	RISQUES			Bonnes Pratiques de Contrôle Interne	Techniques d'Audit
		Facteurs (Scénarios d'empêchement)	Points de contrôle	Impacts		
Infrastructures	S'assurer qu'un site de repli existe, qu'il est suffisamment équipé et opérationnel rapidement	Absence de site de repli Site de repli non opérationnel rapidement Insuffisance de l'équipement prévu sur le site de repli Site de repli exagérément coûteux	Site de repli et matériel de crise prévus	Impossibilité de déployer les dispositifs de continuité d'activité due à l'absence ou l'indisponibilité du matériel et des infrastructures nécessaires	Infrastructures de secours ou site de repli	Vérification de l'existence d'un site de repli et revue de son équipement (suffisance, adéquation avec les besoins en continuité, qualité et maintenance) Evaluation de la pertinence des ressources et moyens déployés pour le site de repli Test effectif du site de repli via une simulation de sinistre
Système d'information	S'assurer de l'existence d'un PSI S'assurer de la sécurisation des données S'assurer de la qualité du matériel informatique	Absence ou mauvaise mise en place d'un PSI Non prise en compte des aspects de sécurité et de protection des données dans la conception du PSI Absence ou mauvaise sensibilisation et formation du personnel Matériel obsolète ou inadapté	PSI formalisé et documenté Matériel informatiques Dispositifs de sécurisation des données	Panne du réseau Absence ou mauvaise protection des informations sensibles ou confidentielles (poursuites juridiques)	Dispositif de continuité du SI efficace et pertinent Système de protection des données en toutes circonstances, en particulier au regard de la confidentialité de celles-ci	Revue de la conception du PSI, et notamment des applications et bases de données identifiées comme critiques, et les dispositifs mis en place pour assurer leur continuité de fonctionnement et d'accessibilité Test d'intrusion dans les systèmes pour accéder ou endommager les données Vérification de l'obsolescence du matériel informatique Revue des cahiers des charges d'acquisition du matériel, et juger de leur correspondance avec les besoins exprimés par le PSI
Alimentation en énergie	S'assurer que des dispositifs pertinents sont prévus et opérants pour garantir la continuité d'alimentation en énergie	Absence ou non pertinence du ou des dispositifs de continuité de l'alimentation en énergie Dysfonctionnements des	Dispositifs de continuité de l'alimentation en énergie Contractualisation	Impossibilité de déployer les dispositifs de continuité qui nécessitent une	Dispositif efficace, pertinent et fiable de continuité de l'alimentation en énergie, tels que la	Revue des dispositifs de continuité de l'alimentation en énergie et tester l'efficacité et la pertinence théoriques Vérifier l'obsolescence, la qualité et

		dispositifs de secours (mauvaise qualité ou mauvais entretien du matériel) Mauvaise contractualisation du recours à des prestataires de secours	des prestataires de secours	alimentation en énergie	redondance des systèmes d'alimentations, des groupes électrogènes ou des prestataires de secours	l'entretien du matériel dédié Vérifier que les dispositifs sont testés régulièrement Tester effectivement les dispositifs de continuité de l'alimentation en énergie via une interruption contrôlée de l'alimentation
Approvisionnements clés	S'assurer que l'organisation a défini et maintient un niveau de stocks de sécurité pertinent pour les approvisionnements clés S'assurer que l'organisation a formalisé et contractualisé un système d'approvisionnements d'urgence auprès de prestataires de secours pour les approvisionnements clés	Mauvaise identification des approvisionnements clés Absence ou mauvaise formalisation ou contractualisation des systèmes d'approvisionnements alternatifs (partenaires de secours) Mauvaise définition des stocks de sécurité par rapport aux besoins en continuité Non maintien du niveau des stocks de sécurité	Stock de sécurité Contractualisation d'approvisionnement d'urgence Dispositifs d'approvisionnement alternatif	Impossibilité de déployer les dispositifs de continuité due à l'absence ou l'indisponibilité du matériel nécessaire Impossibilité de réparer du matériel endommagé due à l'absence ou l'indisponibilité de pièces de rechange	Dispositif de continuité d'activité en cas d'interruption des approvisionnements clés (de puces électroniques notamment), tels que des stocks de sécurité ou un système d'approvisionnement alternatif via des prestataires de secours	Revue du mode de définition des stocks de sécurité Evaluation du niveau des stocks de sécurité Test sur les stocks clés pour s'assurer qu'ils sont au-dessus du minimum de sécurité Revue des contrats d'approvisionnements d'urgence avec les prestataires de secours (type de produits concernés, délais de réactivité, tarification…)
Ressources humaines	S'assurer que l'organisation a prévu et contractualisé le recours à du personnel de secours (intérimaires, détachement du personnel de partenaires…) S'assurer que l'organisation a prévu des outils de travail à distance	Décès ou maladie grave d'une part importante du personnel Impossibilité pour le personnel de se rendre sur son lieu de travail	Contractualisation du recours à du personnel de secours Planning et astreintes Dispositifs logistiques de crise (acheminement du personnel, outils de travail à distance…)	Indisponibilité du réseau Impossibilité de déployer les dispositifs de continuité due à l'absence ou l'indisponibilité du personnel nécessaire	Dispositif de continuité d'activité en cas d'indisponibilité de tout ou partie du personnel	Revue des contrats avec les agences d'intérim pour le recours à du personnel de secours (profils et compétences prévus, délai de réactivité, tarification…) Evaluation des outils de travail à distance prévus par l'organisation (pertinence, complétude de l'accès aux applications et aux données, sécurisation, matériel adapté…)

Conclusion

La réalité des PCA en quelques chiffres

A travers l'étude de benchmark réalisée, s'ajoute aux entretiens individuels avec des professionnels de secteurs d'activités clés la diffusion d'un questionnaire anonyme et succinct, résumant les tendances de la mise en place, du maintien en condition opérationnelle et du pilotage des PCA et de la gestion de crise. Celui-ci a été diffusé à des entreprises de différents secteurs d'activité, via le Club de Continuité d'Activité et le réseau des étudiants de l'IAE d'Aix en Provence.
Une trentaine de responsables de la mise en place de la continuité d'activité ont partagé les pratiques de leur organisation, représentant de nombreux secteurs d'activité : Bancaire, assurantiel, organisations multilatérales, industries chimiques et de manufacture, BTP, transports, alimentaire, énergie, collectivités territoriales, télécommunications…

Ces éléments de données permettent une vision empirique des pratiques réelles des organisations en matière de continuité d'activité.

Il est notamment identifié que 93% des organisations interrogées disposent d'un PCA en place dans leur organisation, et 80% ont prévu un dispositif ou une cellule de gestion de crise. Par ailleurs, 92% ont également un volet spécifique à la continuité informatique ou PSI, qui apparaît ainsi être un aspect incontournable du dispositif.
79% d'entre elles ont en outre prévu un site de repli utilisateur, une statistique qui prouve également l'importance grandissante des PCA dans la stratégie globale de management des risques des entreprises tous secteurs confondus. Les sites de repli utilisateurs étant très onéreux, cela démontre un réel déploiement de moyens par la Direction Générale.
Il est également noté 71% des répondants à notre questionnaire ont intégré une démarche d'audit des PCA.
Nous constatons donc que les PCA et la gestion de crise sont des problématiques essentielles, au cœur des préoccupations des dirigeants d'aujourd'hui. Elles sont prises de plus en plus au sérieux par les organisations, dans une démarche parfois totalement volontariste, puisque 20% des répondants ont déclaré que leur organisation n'était pas dans l'obligation de mettre en place un dispositif de continuité d'activité ou de gestion de crise.
Pour les 80% d'organisations pour qui la mise en place d'un PCA est imposée par un cadre règlementaire, les textes applicables sont notamment Solvency II pour le secteur assurantiel, le CRBF 97-02 pour le secteur bancaire, et la réglementation SAIV pour les Opérateurs d'Importance Vitale.
La volonté à la fois des organisations de déployer ce type de solutions, et du régulateur de l'encourager, peut s'expliquer par la réalité de cette nécessité, lorsque les crises apparaissent de plus en plus fréquentes et de plus en plus graves. Ainsi, 50% des entreprises interrogées ont déjà vécu une crise nécessitant l'enclenchement du dispositif de gestion de crise ou des PCA. Dans 70% des cas les dispositifs en place se sont révélés efficaces.

Il apparaît que la mise en place de la continuité d'activité au sein des organisations est généralement gérée par une cellule dédiée à la continuité d'activité, et sous l'égide du responsable de projet (ou RPCA). Dans la majorité des cas (76% des répondants), le PCA est gouverné par le Comité de Pilotage.

92% des organisations concernées ont par ailleurs affirmé disposer d'une cellule de gestion de crise identifiée.
Pour 69% des organisations considérées, cette mise en place s'appuie sur des normes, mais également sur des référentiels pour 46% d'entre elles, sur la législation pour 54% et à des retours d'expérience de crises passées pour 54%. Seulement 7% de l'échantillon ont fait appel à un organisme externe.
Dans le cas des 30 répondants considérés, 43% des PCA sont certifiés. La tendance est à la hausse, puisque de nombreux RPCA interrogés s'intéressaient à l'obtention d'une certification concernant leur continuité d'activité, notamment relative à la norme ISO 22301 à propos de la mise en place d'un PCA.
Pour ce qui est des outils de mise en place de la continuité d'activité, beaucoup d'entreprises ont mentionné le progiciel PARAD de gestion des PSI. Pour les autres composantes du PCA, 43% d'entre elles ont des outils dédiés à la continuité et gestion de crise majoritairement développés en interne.
Les principales étapes de mise en place des PCA suivies par ces entreprises sont cohérentes avec les bonnes pratiques que nous avions identifiées dans la première partie du présent mémoire.

Parmi les points de contrôle clés soulevés par les bonnes pratiques, on remarque notamment que l'implication de la Direction Générale dans la démarche demeure mitigée. La direction s'engage volontiers dans la mise en place et la réflexion sur les risques critiques et les solutions à envisager, cependant les moyens déployés restent insuffisants de l'avis des responsables PCA.
La totalité des répondants déclare cependant qu'un dispositif de communication interne est prévu. Dans la moitié des cas, celui-ci s'adresse à l'ensemble des collaborateurs de l'organisation, et pour 42% des organisations, il est également spécifique auprès des acteurs PCA. La communication interne se formalise via des e-mails, des communiqués, l'intranet, les formations, des réunions et le reporting, ou encore des campagnes de sensibilisation.
En résultat, les PCA sont globalement perçus comme une démarche essentielle et d'utilité réelle pour l'entreprise par les collaborateurs. Cependant, plusieurs RPCA précisent que l'intérêt qui leur est porté se limite souvent aux contextes de crises.
En ce qui concerne la communication externe, très peu d'organisations la prévoient en amont de la survenance des crises. Dans 70% des cas, elle a lieu seulement en période de crise, et sert essentiellement à rassurer les collaborateurs et parties prenantes, et à sauvegarder l'image de l'organisation.
Enfin, les facteurs clés de succès d'une démarche PCA identifiés par les participants portent sur la transparence, la bonne identification des risques critiques, pour certains il s'agit de bon sens et d'adaptabilité, mais tous sans exception ont parlé d'un engagement sincère de la Direction Générale dans la stratégie de continuité comme ingrédient de base de la réussite du dispositif.

Les grands constats qui se dégagent de nos analyses sont que la continuité d'activité est une problématique qui intéresse les organisations, que les démarches pour la mettre en place existent, qu'elles se développent et s'améliorent de plus en plus, mais qu'elles restent encore largement perfectibles.

Conclusion générale et perspectives

Le succès des démarches de continuité d'activité n'est toutefois possible que si les entreprises et organisations prennent enfin conscience qu'au-delà du coût de mise en place de solutions de continuité, c'est une préservation de ressources bien plus importante au moment de la survenance d'un sinistre grave, une assurance pour l'avenir.

Nul ne peut nier la probabilité grandissante de survenance d'une catastrophe. Dans un monde qui évolue sans cesse, un contexte économique difficile et un environnement politique et écologique instable, les menaces sont multiples et semblent toucher de plus en plus durement les organisations.

Il est certain que les organisations ne peuvent plus se permettre de penser ou d'agir comme vingt ans auparavant : Aucune entreprise n'est intouchable, et c'est en gardant cela en tête que les dirigeants de demain devront décider de la place qu'ils allouent à la stratégie de continuité.

De leur engagement dépendra peut être la survie ou non de leur activité.

Annexes

Annexe 1 – Sources documentaires

Supports de formation

Formation IFACI : Se former à l'Audit Interne
Audit du Plan de Continuité d'Activité – PCA
(Méthodologie déposée propriété du cabinet MICA)

Ouvrages

Plan de Continuité d'activité et Système d'Information, vers l'entreprise résiliente (2ème édition)
Auteur : Mathieu BENNASAR
Editeur : DUNOD, Paris, 2010

Articles et publications

Colloque IFACI – 21 Mars 2012
Continuité d'Activité, Continuité Informatique et Gestion de Crise

Cahier de la recherche IFACI – 2008
Une démarche d'audit de Plan de Continuité d'Activité (PCA)

Le plan de continuité d'activité : Enjeux et Méthodes de mise en place (24/03/2010)
Auteurs : Nicolas Caproni & Mélanie Vignaud
Publié sur : www.cyber-securite.fr
(Sur la base de l'ouvrage de M. Bennasar)

Continuité des activités – ISO 22301 – Quand tout va très mal (18/06/2012)
Auteurs : Stefan Tangen & Dave Austin
Publié sur : www.iso.org

Communiqué de presse : Publication de la norme ISO 22301, le nouveau standard international de management de la continuité d'activité, (15/05/2012, Canada)
Auteur : PECB (Professional Evaluation and Certification Board)
Publié sur : www.pebc.org

Normes, lois et règlements

- CRIPP (Cadre de Référence International des Pratiques Professionnelles) de l'Audit Interne
- Guide SGDSN pour réaliser un plan de continuité d'activité
- Circulaire n°6600/SGDSN/PSE/PPS du 26 Septembre 2008 : Instruction Générale Interministérielle relative à la sécurité des activités d'importance vitale (SAIV)

- Arrêté du Premier Ministre du 2 Juin 2006 fixant la liste des Secteurs d'Activités d'Importance Vitale et désignant les ministres coordonnateurs desdits secteurs, modifié par l'arrêté du 3 Juillet 2008
- Code de la Défense (Article R. 1332-2 et suivants)

Normes ISO

ISO 22301 (Continuité d'Activité)
ISO 27031 (Continuité Informatique)
ISO 22000 (Secteur Alimentaire)

Banque et assurance

- Règlement CRBF 97-02
- Solvency II
- Code Monétaire et Financier

Santé publique

- Circulaire n° DHOS/CGR/2006/401 du 14 Septembre 2006 relative à l'élaboration des plans blancs des établissements de santé et des plans blancs élargis
- Plan blanc et gestion de crise : Guide d'aide à l'élaboration des plans blancs élargis et des plans blancs des établissements de santé
  Edition 2006, annexe à la circulaire n°DHOS/CGR/2006/401 du 14 Septembre 2006
- L'établissement de Santé en Tension : Fiches de recommandations sur le plan blanc et la gestion de crise, suite au séminaire du 23 Septembre 2005.
- Instruction n°DGOS/MSIOS/2013/62 du 21 Février 2013 relative au guide méthodologique pour l'auditabilité des systèmes d'information dans le cadre de la certification des comptes des établissements publics de santé.

Alimentaire

- Règlement Européen n°178/2002 du Parlement européen et du Conseil du 28 Janvier 2002, établissant les principes généraux et les prescriptions générales de la législation alimentaire, instituant l'Autorité Européenne de Sécurité des Aliments et fixant des procédures relatives à la sécurité des denrées alimentaires
- Directive Européenne n°93/43/CEE du Conseil du 14 Juin 1993, relative à l'hygiène des denrées alimentaires
- Guide du gouvernement : Guide d'aide à la gestion des alertes d'origine alimentaire

Energie

- Articles L. 1332-1 à L. 1332-7 du code de la défense ;
- Articles R. 1311-39 à R. 1311-43, R. 1332-1 à R.1332-42, et R. 1421-1 du code de la défense
- Articles D. 1332-39 à D. 1332-41 du code de la défense ;

- Arrêté du Premier ministre du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs, modifié par l'arrêté du 3 juillet 2008 ;
- Arrêté du Premier ministre du 12 mars 2007 pris pour l'application du 1° et du 2° de l'article 12 du décret n° 2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale ;
- Arrêté du Premier ministre n° 10166/SGDN/PSE/CD du 27 avril 2007 portant approbation du plan-type de plan de sécurité d'opérateur d'importance vitale ;
- Arrêté du Premier ministre du 27 septembre 2007 portant approbation du plan-type de plan particulier de protection (PRMD0766738A) ;
- Arrêté du Premier ministre du 27 septembre 2007 portant approbation du plan-type de plan de protection externe (PRMD0766625A) ;
- Circulaire du Premier ministre n° 5152/SG du 5 mai 2006 relative à la mise en œuvre du nouveau régime de sécurité des activités d'importance vitale.

Transports

- Code des Transports (Version consolidée au 18 Juillet 2013)
- Code de l'Aviation Civile (Version consolidée au 30 Juin 2013)
- Ordonnance n° 2010-1307 du 28 Octobre 2010 relative à la partie législative du code des transports
- Directive Européenne n°2003-42 du 13 Juin 2003 relative aux comptes rendus d'événements dans l'aviation civile
- Loi n°2012-375 du 19 Mars 2012 (Loi Diard) relative à l'organisation du service et à l'information des passagers dans les entreprises de transport aérien de passagers et à diverses dispositions dans le domaine des transports
- Arrêtés du 4 Avril 2003 et du 17 Août 2007 fixant la liste des évènements et incidents de l'aviation civile devant être portés à la connaissance du BEA
- Engagements auprès du CGEDD (Conseil Général de l'Environnement et du Développement Durable) du 14 Novembre 2011 relatifs aux dispositifs de viabilité hivernale
- Guide DGAC (Direction Générale de l'Aviation Civile) : Notifier un incident (Janvier 2008)

Télécommunications

- Directives Européennes du 7 Mars 2002 : Cadre
  Autorisations
  Accès
  Service universel
- Directive du 12 Juillet 2002 : Données personnelles
- Directive Européenne du 16 Septembre 2002 : Concurrence
- Loi du 31 Décembre 2003 relative aux obligations de service public des télécommunications et à France Télécom
- Loi du 21 Juin 2004 pour la confiance dans l'économie numérique
- Loi du 9 Juillet 2004 relative aux communications électroniques et aux services de communications audiovisuelles

- Code des Postes et des Communications Electroniques (CPCE)

Sites Internet

Sites gouvernementaux

http://www.legifrance.gouv.fr (Législation Française)
http://europa.eu (Législation Européenne)
http://www.sante.gouv.fr
http://www.developpement-durable.gouv.fr
http://www.economie.gouv.fr
http://www.sgdsn.gouv.fr (Secrétariat Général de la Défense et de la Sécurité Nationale)
http://galateepro.agriculture.gouv.fr/ (Direction Générale de l'Alimentation – DGAL)

Associations professionnelles, cabinets externes & organismes de certification

IFACI (Institut Français de l'Audit et du Contrôle Internes) http://www.ifaci.com
Club de la Continuité d'Activité http://www.clubpca.eu
ISO (Organisation Internationale de la Normalisation) www.iso.org
AFNOR (Association Française de Normalisation) http://www.afnor.org
PECB (Professional Certification and Evaluation Board) www.pebc.org
Cabinet Adenium http://www.adenium.fr
Cabinet Altair Conseil http://www.altairconseil.fr
Cabinet Vision Solutions (continuité informatique) http://www.visionsolutions.com
CNPP (Centre National de Prévention et de Protection) http://www.cnpp.com

Instances de tutelle

HAS (Haute Autorité de Santé) http://www.has-sante.fr
ARCEP (Autorité de Régulation des Communications Electroniques et des Postes) http://www.arcep.fr
AMF (Autorité des Marchés Financiers) http://www.amf-france.org
Comité de Bâle http://www.bis.org/bcbs/

Blogs et journaux en ligne

http://www.lemonde.fr
www.cyber-securite.fr
www.journaldunet.com

Wikipédia

http://fr.wikipedia.org

Annexe 2 – Glossaire

Continuité d'Activité : Absence d'interruption des activités critiques d'une organisation lors de la survenance d'un sinistre venant la priver de son environnement normal de travail, et maintien d'un niveau de service minimum en mode dégradé

Gestion de Crise : Dispositif de continuité d'activité, qui regroupe la veille des indicateurs d'activité visant à détecter et anticiper la survenance d'un sinistre, l'alerte et l'escalade lorsqu'un potentiel sinistre est détecté, l'accompagnement et la gestion de la crise ainsi que de la communication de crise, puis l'accompagnement à la sortie de crise, le retour à une situation normale et le retour d'expérience sur la crise

Plan de Continuité d'Activité : Ensemble des dispositifs de continuité d'activité regroupés dans un même plan ; Il se subdivise en PCA et PRA métiers pour les activités critiques, PCA et PRA fonctions supports, PSI, gestion de crise et une organisation globale qui coordonne ces composantes et assure la sécurité et la logistique

Plan de Reprise d'Activité : Dispositif de continuité d'activité permettant la sortie de crise et du mode dégradé et le retour à un environnement normal de travail

Plan de Sauvegarde Informatique : Dispositif de continuité d'activité permettant d'assurer la continuité informatique, et notamment celle des applications et bases de données critiques, ainsi que les systèmes de télécommunications essentiels ; Il constitue un support aux PCA et PRA métiers et fonctions support en leur fournissant un outil de travail

Risques "Causes" : Il s'agit des risques d'occurrence des sinistres de grande ampleur, tels que les catastrophes naturelles, les sinistres technologiques, les sinistres sociaux, économiques et politiques, les crises sanitaires ou les sinistres nucléaires, radiologiques ou chimiques.

"Conséquences" : Ce sont les risques d'impacts des sinistres de grande ampleur, leurs potentielles conséquences sur les organisations, pouvant les priver de leur environnement normal de travail.

Scénarios d'empêchement : Il s'agit des risques dont la survenance peut empêcher une organisation de mettre en place les points de contrôle clés de la continuité d'activité

Impacts des points de contrôle clés : Ce sont les risques d'impacts pour une organisation de la non mise en place des points de contrôle clés de la continuité d'activité.

Incident : Survenance d'un problème ou d'une anomalie de faible ampleur, dont les conséquences sont limitées et qui peut être traité sans déclencher de situation de crise ; Non traité, un incident peut se transformer en sinistre

Sinistre : Incident de grande ampleur, pouvant avoir des conséquences importantes, et dont la gestion passe par le déclenchement d'une situation de crise et d'un dispositif de continuité d'activité

Crise : Trouble important dans le fonctionnement normal de l'organisation

Robustesse : La robustesse d'une organisation est sa capacité à éviter la survenance d'un sinistre

Résilience : La résilience d'une organisation est sa capacité à survivre et résister aux impacts d'un sinistre, et notamment à assurer la continuité de ses activités critiques à leur niveau de service minimum

Parties Prenantes (Partenaires) : Il s'agit de toutes les structures externes à l'organisation qui ont un intérêt à la continuité d'activité de cette organisation ; On compte notamment parmi elles les clients, les fournisseurs, les banques et investisseurs, les actionnaires, le personnel, les partenaires contractuels ainsi que l'Etat et les instances de tutelle

Service Public : Activité d'intérêt général, assurée par un organisme public ou privé soumis aux règles qui sortent du droit commun

Service Vital : Activité ayant trait, de manière difficilement substituable ou remplaçable, à la production et la distribution de biens ou de services indispensables

Environnement Normal de Travail : Situation habituelle de l'organisation, dans laquelle elle dispose de l'ensemble de ses infrastructures, matériel, outils, personnel… qui sont nécessaires à son activité quotidienne

Activité Critique : Activité ne pouvant subir une interruption prolongée

Site de Repli : Site de travail alternatif d'une organisation, lui permettant de déporter ses activités critiques vers ce site en cas d'indisponibilité du site principal suite à un sinistre

Annexe 3 – Répertoire des Acronymes

ACP	Autorité de Contrôle Prudentiel
ADP	Aéroports de Paris
AMF	Autorité des Marchés Financiers
AFNOR	Association Française de Normalisation
AI	Audit Interne
ARCEP	Autorité de Régulation des Communications Electroniques et des Postes
BEA	Bureau d'Enquête et d'Analyse pour la Sécurité de l'Aviation Civile
BS	*British Standards* (Normes Britanniques)
CA	Conseil d'Administration / Continuité d'Activité
CCA	Correspondants Continuité d'Activité
CCP	*Critical Control Point* (Points de Contrôle Critiques)
CE	Communauté Européenne
CEE	Communauté Economique Européenne
CGEDD	Conseil Général de l'Environnement et du Développement Durable
CH (U)	Centre Hospitalier (Universitaire)
CHSCT	Comité d'Hygiène, de Sécurité et des Conditions de Travail
CI	Contrôle Interne
CNPP	Centre National de Prévention et de Protection
COMEX	Comité Exécutif
CPCE	Code des Postes et des Communications Electroniques
CRBF	Comité de Règlementation Bancaire et Financière
CRIPP	Cadre de Référence International des Pratiques Professionnelles
DG	Direction Générale
DGAC	Direction Générale de l'Aviation Civile
DGAL	Direction Générale de l'Alimentation
DGCCRF	Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes

DGOS	Direction Générale de l'Offre de Soins
DHOS	Direction de l'Hospitalisation et de l'Organisation des Soins (Devenue DGOS en 2010)
DICT	Disponibilité, Intégrité, Confidentialité, Traçabilité des SI
DIVA	Données d'Importance Vitales (Base de données SGDSN)
DM	Dispositif Médical
DMIA	Délai Maximum d'Interruption Acceptable
DRH	Direction des Ressources Humaines
DSI	Direction des Systèmes d'Informations
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité (SI)
HACCP	*Hazard Analysis Critical Control Point* (Analyse des Dangers et Points de Contrôle Critiques)
HAS	Haute Autorité de la Santé
IFACI	Institut Français de l'Audit et du Contrôle Internes
ISO	*International Standardization Organization* (Organisation Internationale de Normalisation)
MEHARI	Méthode Harmonisée d'Analyse de Risques (SI)
MR	Management des Risques
NIMS	*National Incident Management System* (Système National de Gestion des Incidents)
OACI	Organisation de l'Aviation Civile Internationale
OGM	Organismes Génétiquement Modifiés
OIV	Opérateurs d'Importance Vitale
ORSEC	Organisation des Secours (plan d'urgence)
PCA	Plan de Continuité d'Activité
PECB	*Professional Evaluation and Certification Board* (Comité d'Evaluation et de Certification Professionnelle)
PMDT	Perte Maximum de Données Tolérable
PPRI	Plan de Prévention du Risque Inondation
PRA	Plan de Reprise d'Activité
PSEE	Prestations et Services Essentiels Externalisés
PSI	Plan de Sauvegarde Informatique

RATP	Régie Autonome des Transports Parisiens
RFF	Réseau Ferré de France
RPCA	Responsable du Plan de Continuité d'Activité
RPSI	Responsable du Plan de Sauvegarde Informatique
RSSI	Responsable du Système de Sécurité Informatique
SA	Société Anonyme
SAIV	Sécurité des Activités d'Importance Vitale
SAMU-SMUR	Service d'Aide Médicale Urgente Service Mobile d'Urgence et de Réanimation
SGDSN	Secrétariat Général de la Défense et de la Sécurité Nationale
SI	Système d'Informations
SIH	Système d'Informations Hospitalier
SIMCA	Système d'Information du Management de la Continuité d'Activité
SNCF	Société Nationale des Chemins de Fer
SSI	Système de Sécurité Informatique
UE	Union Européenne

Annexe 4 – Comptes-rendus des entretiens de Benchmark

Secteur d'Activité	Ref.
Continuité d'Activité	CR N°1
Bancaire	CR N°2
Santé Publique	CR N°3
	CR N°4
	CR N°5
Energie	CR N°6
Transport	CR N°7
Télécommunications	CR N°8
Industrie Automobile	CR N°9
Finances Publiques	CR N°10
Organisation Internationale	CR N°11

Mémoire : Guide d'Audit des PCA **N°1**
M. Derrahi & J. Garcia

Compte-rendu d'entretien de Benchmark

Secteur d'activité : **Continuité d'Activité**

Fonction :	Secrétaire
Périmètre d'Intervention :	Organisation entière
Rattachement Hiérarchique et Fonctionnel :	Présidence

Mise en Place de la démarche de Continuité d'Activité

L'objectif du PCA est de gérer les conséquences d'une crise. La limite du risque d'occurrence n'entre pas dans le cadre de cette démarche, elle se gère au quotidien. Les raisons qui ont causé le sinistre importent donc peu, ce sont ses conséquences qui sont intéressantes ici.
La continuité d'activité est une préparation à froid, sans les aspects émotionnels, afin d'être en mesure de gérer à chaud. La gestion de crise, quant à elle, consiste à gérer à chaud, et constitue la période d'incertitude avant l'enclenchement de la continuité d'activité. Elle va par exemple prévoir la manière de contacter l'ensemble des employés si un sinistre survient durant le week-end.
La continuité d'activité vise à prémunir une organisation contre des risques majeurs susceptibles de causer sa perte, qui sont essentiellement des risques pénaux, juridiques, financiers graves ou d'image.
La robustesse d'une organisation est sa capacité à éviter la survenance d'un sinistre, tandis que sa résilience est sa capacité à survivre et résister aux impacts de ce sinistre.
La frontière n'est pas toujours très claire entre les activités de maîtrise des risques, de continuité d'activité et de gestion de crise.
La continuité d'activité commence par changer les comportements, puis elle change l'organisation.
Il est nécessaire d'intégrer la dimension humaine dans les PCA. En effet, l'EBITDA demeure le centre des préoccupations, malgré une volonté d'intégrer aux réflexions une certaine déontologie et de l'éthique.
Pour beaucoup d'organisations, le PCA est une obligation et est donc mis en place, mais elles n'y croient pas.
Il faut différencier une crise d'un incident et la dimension stratégique de la dimension opérationnelle.

Risques génériques

Le risque de malveillance ou d'erreur humaine est souvent sous-estimé.
Il est important de gérer le post-crise, de rassurer les clients et rétablir l'image, ce qui engendre des actions marketing.

Risques spécifiques sectoriels

Sans que l'on s'intéresse aux causes, ce sont les conséquences des sinistres qui intéressent la continuité d'activité. Les différents secteurs d'activités ont chacun leurs risques spécifiques :

- Energie : Interruption de l'alimentation en gaz par la Russie
- Alimentaire : Rupture des approvisionnements en matières premières ou en énergie, crise sanitaire sur les produits (clients malades voire morts, baisse du chiffre d'affaires et de la productivité… Ces risques sont gérés par les services Juridique ou Communication), arrêt prolongé de la production
- Télécommunications : Interruption des services sensibles (secours)
- Banque : Coupure d'électricité prolongée (catastrophique pour les traders)

Dispositifs de continuité

A titre d'exemple, pour pallier une interruption de l'alimentation en énergie, une organisation peut prévoir des groupes électrogènes ou déporter sa production vers un autre site.

Mémoire : Guide d'Audit des PCA **N°2**
M. Derrahi & J. Garcia

Compte-rendu d'entretien de Benchmark

Secteur d'activité : Etablissement de crédit - Banque

Fonction :	Responsable du Plan de continuité d'Activité (RPCA)
Périmètre d'Intervention :	Organisation entière
Rattachement Hiérarchique et Fonctionnel :	1/ Direction des Contrôles Permanents et Risques 2/ Direction Générale
Historique du service PCA :	Entre 2002 et 2005

Mise en Place de la démarche de Continuité d'Activité

L'entreprise possède une démarche de continuité d'activité conformément à l'article 4 du CRBF 97-02 modifié. C'est une obligation légale en tant qu'établissement financier que de garantir la continuité de ses services. Il existe également un dispositif de gestion de crise en interne incluant notamment un site de repli en cas d'incapacité du personnel à accéder aux locaux. L'entreprise n'est cependant pas certifiée.

Le RPCA s'est appuyé sur la cartographie des risques opérationnels pour mettre en place le PCA. Il a également tenté de hiérarchiser les activités critiques afin de sélectionner les profils clés des acteurs de la continuité d'activité.

Le plus gros volet de la continuité dans le bancaire étant bien sûr les SI, le PSI de l'entreprise constitue sa priorité en cas de crise majeure.
Les SI sont par conséquent testés régulièrement et un poste est dédié à la continuité informatique, indépendamment du RPCA.

Les PCA sont régulièrement audités par l'Inspection Générale ainsi que les instances de tutelle telles que l'ACP.

Un site de repli est également prévu pour accueillir environ 200 profils nécessaires à la continuité (sur 1200 collaborateurs).

Gouvernance de la Continuité d'Activité et de la Gestion de Crise

Il existe une communication interne liée aux PCA mais elle est limitée. Elle se fait majoritairement via l'intranet de la filiale. Les collaborateurs ont également à leur disposition un numéro vert qu'ils peuvent joindre pour signaler un incident grave et donner l'alerte.
La communication externe quant à elle n'est pas anticipée. Elle intervient uniquement en cas de crise et est gérée au niveau du Groupe.

La continuité d'activité au sein de l'entreprise est globalement perçue comme une démarche obligatoire mais très onéreuse (notamment pour ce qui est des sites de repli). Les employés n'y accordent pas plus d'intérêt que cela.

Résumé de l'entretien : Spécificités de l'entreprise et du secteur bancaire

Le RPCA travaille en coopération avec le RSSI et le SSI et avec un correspondant dans chaque service.
La mise en place d'un PCA en banque est une obligation légale imposée par le CRBF 97-02. Ils se font auditer régulièrement par l'inspection générale, ils subissent des contrôles réguliers de la part du Groupe et des contrôles trimestriels de l'ACP.
Le PCA est une obligation également envers les clients qui aiment savoir si l'entreprise en possède un. C'est aussi une obligation des PSEE (Prestations et Services Essentiels Externalisés).
Le RPCA a fait un découpage de l'organisation par activités et non par services ou directions : le PCA touche surtout les activités critiques (financement, recouvrement factoring, SI), qu'on cherche à tout prix à préserver en cas de crise de niveau 3.
Les alertes PCA sont classées en 3 niveaux différents de gravité : le niveau1, 2, et le 3ème

Les niveaux sont les suivants :

- Niveau 1 : Crise légère qui paralyse un étage ou une activité – Déclenchement de la gestion de crise
- Niveau 2 : Crise plus étendue, par exemple qui paralyserait une partie du bâtiment – Gestion de crise
- Niveau 3 : Crise grave, incapacité de poursuivre l'activité dans ces conditions. Ce niveau de crise appelle une réunion du département de la continuité d'activité avec le Comité de Direction qui statue sur le déclenchement du plan de continuité d'activité et / ou du plan de continuité informatique / plan de repli.

Ils ont également calculé que quelle que soit la gravité de la crise, il fallait impérativement pouvoir reprendre l'activité à J+10, car au-delà ce serait dommageable pour la survie de l'entreprise (continuer de pouvoir financer, pouvoir garder le contact avec le client).
La mise en place d'un PCA a un coût qui peut s'avérer très conséquent, dans cette organisation par exemple, les plans de secours nécessitent des activités essentielles. Pour ce faire, des immeubles sont prévus avec des fournitures essentielles à la continuité (chèques, etc.) ayant une capacité totale de 200 personnes, soit une estimation du nombre de profils (ici lorsqu'on parle de profil on ne peut pas raisonner en nominatif mais en termes de compétences) impératifs à la continuité.
Ils se basent sur la méthodologie du Groupe pour la mise en place du PCA dans la filiale, mais surtout et en premier lieu sur la cartographie des risques opérationnels. Avec le concours des

correspondants, ils définissent l'ordre des priorités à donner aux activités critiques. Par exemple, en temps de crise en établissement financier, les activités de contrôles et d'audit sont interrompues. Ils définissent aussi les délais d'interruption maximum admissibles pour ces activités (Exemple : 1 jour à 1 mois ; pour une partie des activités, il y a une nécessité de continuité quotidienne sous peine de faire faillite).

La DPCA travaille avec le RSSI et les moyens généraux, car ce sont ces services qui portent la continuité d'activité en banque. Les correspondants PCA dans chaque ligne métier sont chargés de remonter les risques majeurs en fonction des scenarios de crise exposés et aident à la mise en place des mesures de continuité.

L'ensemble du dispositif de repli est testé annuellement : jeux de rôle avec des scénarios de crise différents à chaque fois et mise en situation en conditions réelles durant une journée.

Il existe dans cette filiale un reporting trimestriel au Groupe. En effet, l'entreprise suit la démarche imposée par le Groupe. Ils donnent quelques *Guide Lignes* mais laissent les filiales gérer plus ou moins leur mise en place et leur maintien comme elles le désirent. Elles se font auditer sur les points essentiels et règlementaires.

Il existe très peu de communication interne quand il s'agit de PCA dans la filiale. La communication externe est quant à elle gérée par le Groupe avec la collaboration de la Direction et de la DPCA.

Un PSEE est lié aux PCA. En effet deux grands acteurs ont le monopole de la fourniture de locaux de secours.

Il existe un journal de bord de crise, le secrétariat de la crise étant l'audit interne. Il s'agit d'un dispositif en place, qui consiste à garder une trace au jour le jour des journées post-crise (notamment pour les assurances et pour le retour d'expérience).

Exemple de crises vécues :

- Inondation en 2012 qui a déclenché une alerte de niveau 2.
- Accident dû aux travaux : un câble a été arraché par des travaux à proximité et cela a coupé toute l'électricité.

Mémoire : Guide d'Audit des PCA **N°3**
M. Derrahi & J. Garcia

Compte-rendu d'entretien de Benchmark

Secteur d'activité : Santé Publique

Fonction :	Responsable Informatique
Périmètre d'Intervention :	Etablissement entier
Rattachement Hiérarchique et Fonctionnel :	Direction Générale

Mise en Place de la démarche de Continuité Informatique et Continuité d'Activité

La démarche de continuité d'activité, et en particulier la continuité informatique, est essentielle dans un établissement de santé. Ce sont des vies humaines qui sont en jeu. Cette démarche, et les dispositifs qui y sont associés, ont donc toujours existé dans les établissements.

Gouvernance de la Continuité d'Activité et de la Gestion de Crise

La continuité d'activité et la gestion de crise d'un établissement de santé sont très règlementées, à la fois par des textes de lois et surveillés par les instances de tutelle (HAS – Haute Autorité de la Santé – notamment).
Les dispositifs sont formalisés par des procédures, et pilotés en interne par le Directeur de l'Etablissement. Ils font l'objet de formation du personnel et de tests réguliers.
Chaque établissement formalise et détaille ses propres procédures, à partir des recommandations de l'HAS.

Spécificités du secteur de la santé publique

Les Systèmes d'Informations présentent des spécificités sectorielles dans la santé publique qu'il faut prendre en compte dans la mise en place des dispositifs de continuité. Il s'agit notamment de la garantie de la confidentialité des informations médicale, à travers la sécurité des données et des accès informatiques. Le dossier patient, le réseau, et certaines applications critiques doivent en outre être en permanence accessibles, afin de se prémunir contre toute erreur médicale potentiellement préjudiciable pour le patient.
La continuité des télécommunications est également critique, puisque leur interruption peut, par exemple, empêcher les services de secours de prévenir l'établissement de l'arrivée de blessés, qui ne pourra alors pas préparer son arrivée pour un traitement dans les meilleures conditions.
En termes d'activités critiques dont il est essentiel de garantir la continuité d'activité, notre interlocuteur identifie la continuité de fonctionnement du matériel biomédical, la continuité des

services techniques (alimentation en énergie et fluides notamment) et la continuité des approvisionnements clés (médicaments critiques, sang, consommables de première nécessité). Il souligne également l’importance des plans d’urgence de type plan blanc ou d’intégration dans les dispositifs globaux pour que l’établissement puisse réagir à un afflux massif de victimes résultant d’un sinistre externe.

Les différents dispositifs d'urgence (plans blancs ou rouges) font l'objet de simulations soit internes, soit pluri-établissements sur recommandation du préfet.

Mémoire : Guide d'Audit des PCA **N°4**
M. Derrahi & J. Garcia

Compte-rendu d'entretien de Benchmark

Secteur d'activité : **Santé Publique**

Fonction :	Ingénieur Biomédical
Périmètre d'Intervention :	Etablissement entier
Rattachement Hiérarchique et Fonctionnel :	Direction des Services Economiques

Continuité de fonctionnement du matériel biomédical

Mise en Place de la démarche de continuité de fonctionnement

Si une panne de DM (Dispositif Médical) survient, celle-ci peut provoquer un report d'intervention, de rendez-vous… etc. Un problème grave préjudiciable pour le patient peut se produire si la panne survient en cours d'intervention. Les risques portent sur tous les secteurs critiques (ventilateurs, défibrillateurs… etc).
Une procédure dégradée est formalisée pour garantir la continuité d'activité en cas de défaillance d'un équipement biomédical. Elle a été mise en place par le service biomédical et le service qualité, imposée par les décrets de l'HAS du 3 Octobre 1995 et du 5 Décembre 2001.
Les dispositifs de continuité préconisés par la procédure sont par exemple une redondance des dispositifs médicaux, un dépannage auprès d'un autre service, une prise de contact avec le constructeur… etc. Pour élaborer cette procédure, ils se sont appuyés sur des normes, la législation, des retours d'expérience, et le forum des technologies biomédicales de l'association d'Ingénieurs Biomédicaux.
Cette procédure est communiquée au personnel via l'intranet. Elle fait par ailleurs l'objet d'un contrôle lors des visites de l'HAS.
A la connaissance de notre interlocuteur, la continuité d'activité ne fait pas l'objet d'une démarche d'audit, mais le service biomédical réalise une enquête de satisfaction des services utilisateurs tous les deux ans.

Gestion de crise en cas de survenance d'un évènement perturbateur

Une organisation et une équipe de gestion de crise sont définies au niveau de la Direction Générale. Il n'y a pas de dispositif de veille au niveau de notre interlocuteur, et les protocoles de communication se situent également à la Direction Générale. Les différents dispositifs de continuité s'intègrent dans une démarche globale de continuité d'activité et de gestion de crise au niveau de l'établissement.

La continuité d'activité est perçue en interne par les agents comme une démarche essentielle pour l'établissement, qui est obligatoire avec une utilité réelle pour l'établissement.
La continuité d'activité et la gestion de crise ne s'appuient pas sur des outils spécifiques particuliers.

Retour d'expérience

L'établissement n'a pas vécu de réelle crise, mais a subi des incidents :

- Panne du scanner, rendant impossible tout examen
- Panne d'une table d'intervention, avec pour conséquence le report des interventions

Facteurs clés de succès

Pour notre interlocuteur, les facteurs clés de succès d'un dispositif de continuité d'activité et de gestion de crise sont :

- La communication à l'ensemble de l'établissement
- L'implication de tous à tous les niveaux
- La réalisation de "simulations" et l'auto-évaluation

Mémoire : Guide d'Audit des PCA **N°5**
M. Derrahi & J. Garcia

Compte-rendu d'entretien de Benchmark

Secteur d'activité : **Santé Publique**

Fonction :	Pharmacienne
Périmètre d'Intervention :	Etablissement entier
Rattachement Hiérarchique et Fonctionnel :	Pharmacie

Continuité des approvisionnements

Mise en Place de la démarche de continuité de fonctionnement

Les approvisionnements critiques essentiels au fonctionnement de l'établissement concernent les médicaments d'urgences, les solutions et les dispositifs médicaux. Une interruption de ces approvisionnements peut provoquer une rupture de la continuité des soins, avec un risque vital pour les patients.
Une démarche de continuité des approvisionnements a été prévue et formalisée par la pharmacie, comme l'impose le décret n°2007-1428 du 30 Octobre 2007.
Les mesures prévues par ce dispositif sont :

- Contre le risque de rupture de stock en pharmacie, la détermination d'un seuil de commande, le suivi journalier des livraisons, ainsi que le remplacement par référence de dépannage en cas de rupture de stock
- Contre le risque de rupture de stock dans les services de soin, la mise en place d'une armoire sécurisée (médicaments d'urgence…)

Un niveau de stock de sécurité existe, notamment dans le cadre du plan blanc, défini par les urgentistes. Les seuils de réapprovisionnements sont définis en fonction de la consommation moyenne des produits et des posologies des patients (antidote…).
Pour élaborer ces dispositifs, la pharmacie s'est appuyée sur le référentiel d'une société gérante d'anesthésie (réanimation, cardiologie…), et sur un suivi de l'évolution des possibles ruptures de stocks (notamment pour le contenu des armoires sécurisées).
L'information et la formation dispensée autour de la démarche consiste en une sensibilisation des préparateurs en pharmacie au risque de rupture de stocks (optimisation des commandes, suivi…), ainsi que du personnel des services de soin, notamment pour l'anticipation des besoins pendant les horaires d'ouverture de la pharmacie.
L'établissement détient la certification obligatoire des établissements de santé par l'HAS. Il n'existe cependant pas de démarche d'audit de la continuité d'activité en interne.

Gestion de crise en cas de survenance d'un évènement perturbateur

Une organisation et une équipe de gestion de crise sont définies au niveau de l'établissement. La veille visant à prévoir et détecter la survenance d'un incident est assurée par l'astreinte administrative de l'établissement. Les protocoles de communication ne se situent pas au niveau de la pharmacie. L'ensemble des dispositifs s'intègre dans une démarche globale de continuité d'activité et de gestion de crise pour l'établissement.
La continuité d'activité est perçue en interne par les agents comme une démarche essentielle pour l'établissement.

Mémoire : Guide d'Audit des PCA **N°6**
M. Derrahi & J. Garcia

Compte-rendu d'entretien de Benchmark

Secteur d'activité : Energie

Fonction :	Responsable Gestion de Crise (RGC)
Périmètre d'Intervention :	Organisation entière
Rattachement Hiérarchique et Fonctionnel :	1/ Département Gestion de Crise Continuité d'Activité 2/ Direction Corporate Santé et Sécurité 3/ Direction Générale

Mise en Place de la démarche de Continuité d'Activité

L'entreprise possède bien une démarche de continuité d'activité et de gestion de crise. En effet, l'énergie est considérée comme un secteur vital par l'Etat. L'entreprise a donc l'obligation légale de garantir la continuité de ses activités. Au-delà de cette obligation, le secteur est par ailleurs soumis à des règlementations spécifiques : Il appartient aux OIV (Opérateurs d'Importance Vitale).
La continuité d'activité a été mise en place en interne par notre interlocuteur, pour laquelle il s'est basé sur la législation en vigueur, celle spécifique à son secteur d'activité, ainsi que sur le guide du Secrétariat Général de la Sécurité et de la Défense Nationale. Il s'est aussi basé sur son expérience de crises passées pour adapter son Plan.
L'entreprise n'a pas de certification en France, cependant une filiale à l'étranger est certifiée ISO 22301. Cette entreprise ne possède pas d'outils spécifiques dédiés à la continuité d'activité, à part pour les systèmes de sauvegarde.
Le Responsable Gestion de Crise a suivi les étapes naturelles de la démarche de continuité d'activité à savoir : la désignation d'un responsable en charge de la continuité, la mise en place d'une cartographie des processus et des risques, l'analyse des impacts et conséquence des risques, la sélection des activités critique et leur priorisation, l'élaboration de solutions de secours, la mise en place d'un PSI, le déploiement de ressources et de moyens ainsi que la mise en place d'un site de repli, la formation des parties prenantes (exercices et formation sur les PCA en interne), ainsi que la mise en place d'une cellule de gestion de crise. Les PCA sont par ailleurs régulièrement testés et les dispositifs mis à jour.
Il existe bien entendu une démarche d'audit des PCA au sein de l'entreprise, notamment pour vérifier la conformité du plan aux obligations légales liées aux activités. De plus, une quarantaine de contrôles supplémentaires sont effectués tous les ans sur les dispositifs liés aux PCA.

Un volet spécifique à la continuité informatique a été mis en place, comme souvent dans les grandes structures possédant des architectures de systèmes d'information complexes.

Gouvernance de la Continuité d'Activité et de la Gestion de Crise

L'organe de pilotage du PCA dans cette entreprise est le comité de pilotage. On note aussi l'implication du management dans tous les services.
L'implication de la direction générale existe réellement selon notre interlocuteur. Cette implication et cet engagement sont liés aux différentes crises rencontrées par le passé.
Il y a également bien une cellule de gestion de crise identifiée, sous la responsabilité du RGC.

La DRGC s'occupe également de la communication interne sur la démarche de continuité et de gestion de crise auprès des acteurs concernés par son déploiement et de tous les collaborateurs, ainsi qu'envers le top management.
Cette communication se fait via l'intranet dans le volet santé, sécurité et gestion de crise.

La perception de la continuité a évolué en interne. Aujourd'hui la démarche de continuité d'activité est perçue dans l'entreprise comme utile, voire essentielle pour l'entreprise.
Une démarche de communication externe est également prévue en amont et en aval de la survenance d'une crise. Elle sert à l'entreprise à rassurer les parties prenantes : client, autorités, élus…
La communication externe se formalise sous toutes les formes : communiqués de presse, courriers, RDV individuels ou collectifs.

Spécificités du secteur de l'énergie

Le volet le plus conséquent de la continuité d'activité dans cette entreprise est représenté par les SI, la continuité opérationnelle ne pouvant exister sans SI.

Les risques spécifiques à la distribution du gaz :

- Arrêt subit de l'approvisionnement en gaz liquide des pays fournisseurs.
  Une telle interruption a été vécue deux fois en hiver et,à cette occasion, le dispositif de gestion de crise a été déclenché
- Cas d'explosions de gaz chez les particuliers ou dans les tuyaux de transport du gaz qui sont parfois endommagés par des tiers (travaux, actes de malveillance)
  Cela doit être géré notamment avec les autorités. Lorsque ces cas rares surviennent, ils doivent gérer la continuité de la distribution et la pénurie pour parfois toute une zone d'habitation…
- Défaillance d'installation, coupure de gaz dans un certain périmètre
  Les conséquences sont les mêmes : arrêt de l'approvisionnement qui impose le déclenchement du plan de continuité et la garantie de la sécurité des biens et personnes.

Des exemples de crise :

- Explosion du cours Lafayette à Lyon qui a paralysé un quartier pendant plusieurs années
- Le décès de deux agents de l'entreprise

Ces deux évènements on déclenchés une alerte et la mise en place de la cellule de crise. Une mise en place de communication de crise (presse locale, régionale).

Selon notre interlocuteur, la clé d'un bon dispositif reste l'engagement de la direction.

Mémoire : Guide d'Audit des PCA **N°7**
M. Derrahi & J. Garcia

Compte-rendu d'entretien de Benchmark

Secteur d'activité : **Transport Aérien**

Fonction :	Chargé d'études Risques Crise et Continuité d'Activité
Périmètre d'Intervention :	Organisation entière
Rattachement Hiérarchique et Fonctionnel :	1/ Département Management des Risques et Préventions 2/ Direction de la Sûreté et du Management des Risques 3/ Direction Générale

Contexte de la démarche de Continuité d'Activité

La formalisation et l'organisation de l'ensemble des dispositifs de maîtrise des risques de l'entreprise ont été mises en place à la suite d'une évolution majeure dans le fonctionnement de l'organisation, qui a entraîné un travail important sur la gouvernance. Cela concerne le Management des Risques, le Contrôle Interne, l'Audit Interne et donc la Continuité d'Activité.
Concrètement, il ne s'agit pas d'une démarche nouvelle, puisque l'activité intrinsèque de l'entreprise, ainsi que la règlementation à laquelle elle est soumise, impliquent une préoccupation importante de maîtrise des risques et de continuité d'activité. Il a donc toujours existé de nombreux dispositifs dans l'entreprise, intégrés dans les processus au quotidien. Mais en l'absence d'un organe de supervision transverse, ceux-ci restent imparfaits, incomplets, non homogènes et non coordonnés. De plus, les nombreux intervenants externes ne permettent pas d'avoir une visibilité sur la sécurisation de l'ensemble de la chaîne des processus.

La démarche de notre interlocuteur sur la problématique de continuité d'activité consiste actuellement à la coordination globale des dispositifs, à travers la définition des objectifs de continuité de l'entreprise en accord avec les obligations règlementaires, et notamment le niveau de service minimum requis pour les différentes activités. Le but est de bâtir un référentiel de continuité d'activité.
La prochaine étape consistera en une analyse détaillée des dispositifs de continuité existants par rapport à ce référentiel, qui ne sera pas facilitée par la formalisation très hétérogène de ces différents éléments (dispositifs SI, métiers, clauses dans les contrats des prestataires…).
Enfin, il s'agira d'améliorer et de perfectionner la gestion de la continuité d'activité de l'entreprise.

Démarche Globale de Continuité d'Activité

Stratégie de continuité

Pour définir la stratégie de continuité, il est intéressant de se baser sur les activités pour lesquelles il y a des astreintes et des intérims mis en place dans l'entreprise : ils concernent des activités essentielles pour lesquelles il faut considérer la gestion de la continuité d'activité (activités critiques).
Cette définition s'appuie également sur les obligations règlementaires (en particulier sur la loi DIARD qui fixe le niveau de service minimum à assurer), et la stratégie globale de l'entreprise (objectifs stratégiques).
Les mesures de continuité s'axent sur deux dimensions :

- La robustesse (chercher à éviter la panne ou la crise)
- La résilience (réaction lorsque la panne ou la crise s'est produite, solutions palliatives, limitation des impacts)

Les dispositifs liés à la robustesse sont plus coûteux, mais garantissent une meilleure sécurité.
On distingue par ailleurs 3 niveaux de continuité d'activité :

- La continuité au quotidien (déviations de circulation, traitement des bagages, viabilité hivernale…) qui sont des éléments bien maîtrisés, intégrés aux processus opérationnels ;
- La continuité à long terme, qui consiste à prévoir l'évolution de l'entreprise et l'intégrer dans les projets de développement (lors des constructions d'infrastructures notamment) ;
- Les PCA face aux risques aléatoires et chocs extrêmes, qui visent à assurer la continuité d'activité en mode dégradé, la gestion et la sortie de crise.

Conception des plans

La démarche se base sur des études, et des échanges avec les utilisateurs afin de bien cerner les besoins, les enjeux et le fonctionnement des processus. Il y a également une dimension de vulgarisation des éléments.

Communication

Il n'y a pas de communication globale au niveau de l'entreprise sur la continuité au quotidien (en interne et en externe). La communication en temps de crise est gérée par les cellules de crise.
Il y a eu une communication sur les dispositifs de viabilité hivernale, mais ce cas particulier revêt une grande importance pour l'entreprise, et possède une réelle dimension stratégique, avec une acceptation de l'aléa qui est très faible (Dossiers de presse Service Hivernal, engagement officiel de l'entreprise).
Il y a par ailleurs une démarche de sensibilisation des acteurs, avec l'objectif de leur faire comprendre que les risques existent au quotidien.

Instances décisionnelles

La continuité d'activité implique une prise de décision, notamment en ce qui concerne l'arbitrage budgétaire de mise en place des solutions, en fonction de la réalité économique des impacts et du coût des solutions. Lorsque le Plan de Continuité d'Activité considéré est transverse et stratégique, la décision est prise en COMEX. S'il s'agit d'un plan plus opérationnel, la décision peut être décentralisée.
La légitimité de la démarche de continuité d'activité n'est pas formalisée par une lettre de mission comme peut l'être une mission d'audit et repose aujourd'hui sur la volonté des Directions et Unités Opérationnelles de mettre en place une bonne structure de gestion. A terme, lorsqu'un référentiel

de continuité d'activité sera établi, l'objectif est de s'appuyer sur des missions d'audit pour maintenir les PCA en condition opérationnelle et les optimiser.

Articulation avec les autres dispositifs de maîtrise des risques

La mise en place des PCA opérationnels s'appuie aujourd'hui sur l'aide de l'audit et du contrôle internes, sur la base d'une demande de la Direction Générale ou du Responsable Métier, mais cette démarche n'est pas encore cadrée par des référentiels et des objectifs précis.

Continuité d'Activité Informatique

C'est aujourd'hui l'activité la plus avancée dans la démarche de continuité d'activité de l'entreprise.
Il n'y a pas de différenciation entre un Plan de Secours Informatique (fournir les outils nécessaires au déploiement des PCA métiers) et un PCA informatique (assurer un service informatique minimum en cas de crise informatique). En effet, la DSI a défini un niveau d'activité qu'elle est en mesure de maintenir en tous temps, et c'est sur ces moyens que les métiers vont s'appuyer pour définir leur propre PCA.
Le niveau de service minimum assuré par la DSI est adapté aux besoins opérationnels de l'entreprise : En effet, la DSI a une bonne connaissance de ces besoins, de par l'activité quotidienne. Il y a par ailleurs des systèmes de base dont il est important d'assurer la continuité, puisque les autres systèmes se greffent dessus (réseaux et disponibilité des données notamment).
Lorsque l'informatique subit une crise d'ampleur limitée et fonctionne en mode dégradé, cela n'est pas perceptible par l'utilisateur.

Elaboration du PCA Informatique

Un animateur de la démarche est identifié. Celui-ci a listé tous les systèmes et a cherché à les hiérarchiser en termes de criticité. Il a ensuite rencontré les responsables des différents systèmes pour affiner cette analyse.
Il a élaboré des documents "chapeau", puis a invité chaque responsable à élaborer ses modes opératoires de continuité.
Enfin, un comité de relecture, composé notamment de représentants métiers, a validé ces éléments.
Le PCA informatique est donc bien documenté.

Continuité d'activité en cas de défaillance totale de l'informatique et des télécoms

Dans une entreprise où la plupart des modes opératoires reposent aujourd'hui sur l'outil informatique, l'enjeu majeur de la continuité d'activité réside dans la capacité à travailler privé de cet outil.
Les acteurs des processus critiques sont sensibles à cette problématique, et des modes opératoires alternatifs sont prévus, comme par exemple :

- L'enregistrement passager qui est possible manuellement (même si très long) ;
- Les tours de contrôle qui maintiennent en parallèle les anciens systèmes papiers…

Il reste cependant des activités critiques qui ne peuvent pas se passer des outils informatiques et télécom, c'est par exemple le cas des radars, qui rendent les PCA informatiques particulièrement importants.

Gestion de Crise

Il y a au sein de l'entreprise 3 niveaux de gestion de crise :

- ➔ Un premier niveau au sein des Unités Opérationnelles
  Cette première cellule de crise fonctionne 24h / 24, et se charge de la détection des incidents et de la coordination multi-acteurs et multi-services pour que l'activité continue.
- ➔ Un second niveau dans les Directions (astreinte décisionnelle)
  C'est le niveau des plateformes opérationnelles
- ➔ Un troisième niveau Corporate (Siège)
  Cette cellule de crise coordonne les autres cellules, et se préoccupe des enjeux et des risques liés à la crise pour l'entreprise au niveau global. Elle supervise également la communication (interne et externe) de la crise.

Les cellules de crise sont chargées de détecter les incidents et les crises, de les gérer, et de déclencher les Plans de Continuité le cas échéant. En fonction du périmètre de la crise (UO, Direction ou Corporate), la gestion de crise dépend de l'un ou l'autre des niveaux ci-dessus.

Viabilité Hivernale

L'entreprise a été fortement marquée par l'hiver 2010-2011 et l'importance des épisodes neigeux. Face à un évènement exceptionnel tant en terme de durée que d'intensité, les moyens consacrés habituellement au service hivernal n'ont pas été suffisants.
Suite à cela, des dispositifs très importants ont été mis en œuvre, des engagements officiels ont été pris, et l'ensemble de la démarche a été organisé et formalisé. Aujourd'hui, l'entreprise est particulièrement performante sur ces aspects.

Continuité de l'alimentation électrique

Cette continuité est assurée par un travail sur les deux dimensions de continuité :

- Robustesse : Double réseau électrique, où chacun est capable de supporter l'ensemble de l'activité, mais en situation normale celle-ci est répartie à 50% sur chaque réseau. En cas de défaillance de l'un, l'autre peut aisément prendre le relai ;
  Groupes électrogènes à demeure (maintenus et testés par l'entreprise).
- Résilience : Onduleurs ;
  Contrats avec des prestataires "de secours" chargés de fournir un groupe électrogène en cas de crise (cela implique une préparation, afin d'identifier le prestataire en amont, s'assurer que le prestataire fournira le matériel adapté, s'assurer que les délais d'acheminement sont cohérents avec les délais maximum d'interruption de l'activité acceptables, s'assurer que l'acheminement est possible).

La continuité de l'alimentation électrique est un enjeu majeur pour l'entreprise (balisage, tours de contrôle, affichage…).

Autres éléments de continuité

- Equipes de nuit systématiquement présentes sur les plateformes, même s'il n'y a pas de trafic planifié : La plateforme est toujours en mesure d'accueillir un appareil qui serait en détresse, ou détourné depuis une autre plateforme. Une obligation règlementaire impose cette capacité d'accueil ;
- Accueil passager et stocks "de crise" (fourniture d'hébergement, lits de camp, nourriture, matériel de première nécessité… lors de perturbations importantes des vols) qui portent essentiellement sur la qualité de service et de traitement du passager, et répondent davantage à des problématiques commerciales d'image que de réelle continuité d'activité.

Test et maintenance des Plans de Continuité d'Activité

Un retour d'expérience est fait après une crise, afin d'éviter qu'elle ne se reproduise : Améliorer la robustesse de l'entreprise (c'est le cas par exemple de la viabilité hivernale, dont les dispositifs ont été modifiés après la crise de l'hiver 2010-2011).
Les PCA des processus critiques font l'objet de tests réguliers, dont la fréquence dépend de l'ampleur du test. Pour certains, les tests font partie du quotidien (informatique ou viabilité hivernale par exemple), d'autres sont annuels, trimestriels ou autres (réseau d'alimentation électrique et groupes électrogènes par exemple).
Pour les processus moins critiques, le PCA n'est pas toujours testé régulièrement, en raison de la difficulté à mettre en œuvre le test au regard de l'enjeu (enregistrement passager manuel par exemple). Les clauses de continuité prévues dans les contrats avec les prestataires ne font pas l'objet de tests.

Mémoire : Guide d'Audit des PCA **N°8**
M. Derrahi & J. Garcia

Compte-rendu d'entretien de Benchmark

Secteur d'activité : Communications électroniques

Fonction :	Directeur Missions Infrastructures Vitales
Périmètre d'Intervention :	Organisation entière
Rattachement Hiérarchique et Fonctionnel :	1/ Direction Sécurité Groupe 2/ Direction Générale

Mise en Place de la démarche de Continuité d'Activité

L'entreprise, en tant qu'opérateur de communication a une activité dite vitale et doit légalement assurer l'existence un dispositif de continuité d'activité.
Elle possède par conséquent bien évidemment plusieurs PCA et un dispositif de gestion de crise identifié, comme l'impose la règlementation en vigueur pour ce secteur d'activité.
La continuité d'activité a été mise en place par notre interlocuteur, le directeur chargé des infrastructures vitale.

Pour la mise en place des PCA de l'entreprise, il s'est appuyé sur la Norme 22301, la législation (SAIV) et également sur le retour d'expérience des crises passées.

Tout comme beaucoup de ses confrères gestionnaires de crises, il possède des outils dédiés à la continuité développés en interne avec l'aide des SI.

Les grandes étapes de la démarches de mise en place des PCA ont été respectées ; il s'est en effet appuyé sur les cartographies des risques et des processus, en a dégagé les impacts majeurs, a priorisé les activités critiques, élaboré des solutions de secours, il a déployé les ressources et moyens nécessaires à la continuité (site de repli), et le PCA est testé régulièrement. Tout cela respecte également les prérogatives SAIV (Décret Européen de Sécurité).

Pour faire évoluer et vivre son PCA, l'entreprise a une communauté interne d'une centaine de personnes qui travaillent à sa mise à jour lors de rencontres régulières. Les PCA au sein de l'entreprise sont naturellement audités en interne pour vérification de leur conformité au regard des règlementations en vigueur.
Ils disposent par ailleurs d'un volet spécifique à la continuité informatique et de plusieurs sites de repli.

Gouvernance de la Continuité d'Activité et de la Gestion de Crise

Les comités de pilotage et opérationnel (par PCA) pilotent le dispositif dans l'entreprise. L'implication de la Direction Générale qui était jusqu'à récemment difficile est aujourd'hui totale (elle est notamment due aux différentes crises qui ont secouées l'organisation).
L'entreprise dispose de plusieurs cellules de gestion de crise identifiées.

En ce qui concerne la communication interne, elle existe et elle concerne tous les collaborateurs, et pas seulement les parties prenantes à la démarche de continuité d'activité. Cette communication se formalise PCA par PCA.
Elle a une influence certaine puisque la plupart des collaborateurs voient les PCA comme une démarche réellement utile pour l'entreprise.
Une procédure de communication externe est également en prévue en amont de la survenance de crises graves et en période de crise. Elle a pour but de rassurer les collaborateurs et parties prenantes tout autant que de promouvoir la résilience de l'organisation via des brochures en ligne, ou des communiqués de presses…etc.

Spécificités du secteur d'activité

Les volets les plus importants du PCA dans cette entreprise touchent aux SI (comme pour la plupart des secteurs) mais aussi à la continuité opérationnelle : plus précisément aux services de communications électroniques.

Les risques métiers spécifiques à l'entreprise :

- Absence d'énergie
- Pénurie de puces électroniques
- Manque de personnel

Ils ont de nombreux exemples d'incidents :

- Les tempêtes, typhons…
- Une panne totale du réseau

Mais le PCA en place c'est toujours révélé utile en cas de crise.
Enfin, notre interlocuteur conclut en précisant que le secret d'une bon PCA repose dans une bonne communication interne ainsi qu'une bonne organisation interne.

Mémoire : Guide d'Audit des PCA **N°9**
M. Derrahi & J. Garcia

Compte-rendu d'entretien de Benchmark

Secteur d'activité : **Industrie Automobile**

Fonction :	Responsable Veille, gestion de crise et continuité d'activité
Périmètre d'Intervention :	Organisation entière
Rattachement Hiérarchique et Fonctionnel :	1/ Direction prévention et protection 2/ Direction générale

Mise en Place de la démarche de Continuité d'Activité

La démarche de continuité d'activité dans l'entreprise est une démarche encore très jeune et qui se met doucement en place. En effet, ce sont les crises passées et notamment la pandémie grippale de 2009 qui a décidé la direction d'allouer des moyens à la mise en place d'une gestion de crise et d'un plan de continuité.

Il existe plusieurs PCA et dispositifs de gestion de crise par secteurs au sein de l'entreprise, bien que la règlementation en vigueur ou spécifique à ce secteur ne les contraignent pas à le faire.
La continuité d'activité s'est formalisée à l'époque de la pandémie H1N1 en France. Le dispositif a été mis en place par notre interlocuteur de façon plus sérieuse qu'auparavant e avec l'aide de la direction du management des risques.
Ils se sont majoritairement appuyés sur la norme 22 301 relative aux PCA mais aussi sur le retour d'expérience de crises passées. Notre interlocuteur a également fait un Benchmark auprès de ses confrères dans d'autres entreprises pour connaitre les bonnes pratiques en termes de continuité.
Pour la mise en place de la démarche, ils ont par conséquent suivi les grandes étapes de mise en place du plan :

- Cartographies de processus et de risques
- Analyse des conséquences
- Mise en place d'un PSI
- Information aux collaborateurs
- Mise en place d'une cellule gestion de crise
- Et tests

La phase d'élaboration des solutions de secours et le déploiement des ressources qui leur sont allouées est encore en cours d'étude.

L'entreprise ne possède aucune certification relative aux PCA. Ils n'ont pas non plus élaborés un des outils spécifiques à la gestion de crise.

Notre interlocuteur fait aujourd'hui vivre et évoluer le PCA de l'entreprise en reprenant la démarche et en essayant de construire un modèle adapté à son activité, en prenant à la fois en compte la dimension de résilience du site et de l'entreprise.
Le PCA et la gestion de crise ne font pour l'instant pas partie du plan d'audit annuel.
Notre interlocuteur nous précise qu'ils ne disposent pas non plus de sites de repli. Bien qu'il conçoive l'intérêt d'un site de repli, cette solution serait trop onéreuse à mettre en place pour une entreprise de cette envergure.

Gouvernance de la Continuité d'Activité et de la Gestion de Crise

Les organes de pilotage du PCA ne sont pas encore bien définis. Notre interlocuteur est pour le moment le seul décideur avec appui de la présidence de l'entreprise. L'engagement de la direction est plutôt positif puisqu'ils donnent au projet les moyens de se mettre en place, il ne tient qu'à eux de les convaincre qu'il faut qu'ils leur consacrent plus de temps encore.
Ils ont toutefois réussi à mettre en place une cellule de gestion de crise identifiée.

Les communications interne et externe en amont de la survenance de crise, sont pour le moment inexistantes. Ils sont actuellement en cours de réflexion quant à leur mise en place. Les collaborateurs semblent toutefois percevoir le dispositif de gestion de crise et de continuité comme une démarche réelle pour l'entreprise. En effet, notre interlocuteur nous explique que les collaborateurs, comme partout ailleurs, voient très bien l'utilité des PCA et ce particulièrement en période de sinistre : ils voient ce que l'entreprise peut leur apporter à l'instant T. Le reste du temps ce n'est sans doute pas la préoccupation majeure.
Quant à la communication externe en période de crise, elle est selon eux nécessaire pour promouvoir la résilience de l'organisation et rassurer les collaborateurs et parties prenantes. Elle est prise en charge par le service communication dont c'est le travail.

Spécificités du secteur d'activité

Les volets continuité opérationnelle et continuité informatique sont tout aussi important l'un que l'autre dans le PCA de l'entreprise. En effet, dans l'industrie en particulier la continuité opérationnelle prend une grande place, due à la nature des activités. En effet, les risques métiers spécifiques sont surtout liés à la Supply Chain.

Les exemples d'incidents vécus par l'entreprise :

- Evènements au Japon en 2012 : Un partenaire fournisseur a été impacté par la crise, ce qui a eu des conséquences directes sur le constructeur automobile. Du jour au lendemain, l'entreprise s'est retrouvée dans l'incapacité de produire, suite à la rupture de ses approvisionnements. Il y a eu à ce moment-là une véritable prise de conscience de la difficulté de la gestion des risques relatifs à la supply chain et du besoin de les anticiper. Ils ont pris conscience également de l'importance de l'interdépendance avec être tous les acteurs de la chaine de production. C'est là un problème très propre à l'industrie en général

et qui démontre bien l'importance du mode de gouvernance et de pilotage sur les flux et la coordination entre les différents acteurs de la production.

- La pandémie grippale de 2009.
- Les grosses neiges de l'hiver 2012-2013 à Paris.

Le PCA, qui était vraiment opérationnel cette année, s'est révélé très utile, notamment pour ce qui est du dispositif de remontée des alertes. Les fortes intempéries ont paralysé des entrepôts et le dispositif de gestion de crise enclenché, ils ont pu prévenir des collaborateurs le week-end de ne pas faire le déplacement jusqu'aux entrepôts, entre autres, et de mettre en place lorsque cela était nécessaire, le télétravail.

En conclusion, notre interlocuteur nous explique que selon lui, l'un des facteurs clés de la réussite d'un dispositif de gestion de crise est l'implication du pilotage. Il faut qu'il soit le « moteur » numéro un du projet.
Pour ce qui est des risques, il faut selon lui dans un premier temps, avoir une approche en termes de conséquences et d'impacts sur l'organisation pour avoir un PCA efficace. Il faut également le budget car les PCA sont très onéreux à la mise en place et à la maintenance et toutes les entreprises, surtout en ces temps de crise, ne peuvent se le permettre.
Il faut également fonctionner en termes de typologie du risque dans un deuxième temps, car selon l'implantation des sites de production ou des sites de fonctions support, les risques ne sont pas les mêmes.

Mémoire : Guide d'Audit des PCA **N°10**
M. Derrahi & J. Garcia

Compte-rendu d'entretien de Benchmark

Secteur d'activité : **Finances Publiques**

Fonction :	RPCE
Périmètre d'Intervention :	Organisation entière
Rattachement Hiérarchique et Fonctionnel :	1/ Direction des Risques et du Contrôle Interne 2/ Direction Générale

Mise en Place de la démarche de Continuité d'Activité

Il existe donc un PCA au sein de l'organisation. Il en existe même plusieurs (une dizaine environ) puisqu'il y a un PCA par direction opérationnelle. Ils ont également en place un dispositif de gestion de crise La réglementation l'imposant dans leur secteur d'activité.
En effet, en tant qu'établissement de crédit, l'organisation est soumise au CRBF-97 02, mais étant un organisme qui dépend de l'état, ils bénéficient de dispositions particulières.

Pour la mise en place de leur PCA, ils se sont appuyés sur des normes et la législation (97-02, plan de lutte contre la pandémie, PPRI (plan d'inondations en cas de crue de la seine).
L'organisation n'est par ailleurs pas certifiée, tout comme la plupart des établissements bancaires, qui sont contrôlées par des instances de tutelles dont le rôle est de se prononcer notamment sur la fiabilité de leur PCA et sa conformité au regard de la loi.
Ils ont des outils spécifiques à la continuité d'activité ; ces outils ont été développés en interne avec les SI.

Notre interlocuteur a mis en place les PCA en passant par trois grandes étapes :

- Une analyse des risques croisée avec la cartographie des processus
- Un découpage en trois typologies de risques (risques d'immeuble, risque de personnes, risques liés aux SI)
- Elaboration des solutions de secours

Ils ont également mis en place une cellule de gestion de la crise et maintiennent la fiabilité de leur système via des tests réguliers et des mises à jour du dispositif.

Au-delà des audits provenant des organismes de tutelle, ils rendent compte à l'audit interne régulièrement.
Comme chaque établissement bancaire, dont l'organisation de la CDC se rapproche beaucoup en termes de typologie d'activités, les SI sont le vecteur principal de toutes les activités. C'est donc bien là où résident les risques majeurs et c'est naturellement que le volet le plus important de la continuité porte sur le plan de secours informatique.

Il existe, pour répondre à un éventuel cas de sinistre bâtiment grave, un site de repli utilisateur.

Gouvernance de la Continuité d'Activité et de la Gestion de Crise

Le comité de pilotage est l'organe en charge du PCA. Cependant selon notre interlocuteur, l'engagement de la direction serait à optimiser. Ils ne sont concernés par la démarche que l'lorsqu'il y a une crise.

Il existe également une communication interne sur les PCA au sein de l'organisation. Elle touche tous les acteurs concernés par le déploiement de la continuité ainsi que tous les collaborateurs, bien qu'elle soit insuffisante selon notre interlocuteur. En effet, elle se résume à des informations sur l'intranet, des formations non obligatoires et un numéro vert d'alerte en cas de sinistre.
Une communication externe est également prévue en période de crise uniquement, et vise spécifiquement à sauvegarder l'image de l'organisation et rassurer les PSEE et parties prenantes (Porte-paroles, communiqués de presse…)
Cette communication de crise est exclusivement encadrée et gérée par le service communication de l'organisation ; Le RPCA ici ne fait que le relais entre la gestion de crise et la communication, mais ne s'exprimera jamais en public sur le management de la crise.

De manière assez globale, les PCA sont plutôt bien perçus en interne dans l'organisation. En effet, ils sont perçus comme une démarche essentielle pour l'entreprise, une démarche obligatoire mise en place sans davantage de questionnement. La démarche est néanmoins vue également comme du travail supplémentaire et très chronophage.

Spécificités du secteur Public

Le volet le plus important de la continuité d'activité reste les SI. Cela dépend cependant le plus souvent de la typologie de crise, mais des SI dépendent la continuité opérationnelle.
Les risques métiers spécifiques au secteur public et finances sont bien sur les risques liés aux SI et leur architecture puisque l'ensemble des activités génératrices de revenus sont portées par cela. Il s'agit également de manager les problématiques de confidentialité avec beaucoup de soin. Il s'agit ici de ne rien laisser filtrer car les missions sont étatiques et donc confidentielles, ce qui rend la gestion de la crise d'autant plus délicate.

Pour les situations ou exemples de crises, elles sont confidentielles. Cependant il existe des crises dont nous entendons parler tous les jours, et qui sont à la charge de l'organisation. Elle choisit cependant de ne pas communiquer dessus.

Pour finir, selon notre interlocuteur, le facteur clé d’un bon dispositif de PCA et de gestion de crise est avant tout le bon sens.
Il s’agit également de ne pas imposer de restrictions préalables sur le sujet ; Un bon levier à cet égard est l’ACP.

Mémoire : Guide d'Audit des PCA **N°11**
M. Derrahi & J. Garcia

Compte-rendu d'entretien de Benchmark

Secteur d'activité : **Organisation Internationale**

Fonction :	Responsable des méthodes de gestion de crises, des exercices et de la formation des opérationnels
Périmètre d'Intervention :	Organisation entière
Rattachement Hiérarchique et Fonctionnel :	1/ Direction des méthodes de gestion de crise 2/ Direction Exécutive 3/ Direction Générale

Mise en Place de la démarche de Continuité d'Activité

L'organisation a une démarche de continuité d'activité en place ainsi qu'un dispositif de gestion des crises, cependant aucune règlementation relative à son activité ou son secteur ne l'impose. La démarche PCA a été mise en place par la Direction Exécutive de l'entreprise sous l'impulsion du secrétariat général.
Pour sa mise en place, ils se sont appuyés sur un organisme externe (Consulting). L'organisation n'est par ailleurs pas certifiée.

Ils possèdent des outils développés spécifiquement pour la gestion PCA :

- Solutions de gestion de campagnes d'appels (alertes générales et ciblées en fonction des besoins liés à l'évolution de la crise)
- Solutions internes et externes de conservation et de consultation des données sensibles et utiles à la gestion de crise.

Les grandes étapes de la démarche sont relativement génériques à tous les secteurs :

- Croisement de la cartographie des risques opérationnels et des processus
- Priorisation des activités critiques
- Elaboration des solutions de secours en fonction du résultat
- Mise en place d'un PSI
- Mise en place de la cellule de gestion de crise
- Tests

Au sein de la Direction des Méthodes de Gestion de Crise, pour faire vivre le dispositif de continuité d'activité, ont été élaborés des exercices avec retours d'expérience (pour les mises à jour du PCA si besoin), ainsi qu'un Benchmark et des réunions trimestrielles du comité de gestion des crises.

Les PCA ne sont cependant pas audités en interne et aucun site de repli n'a été mis en place pour le moment, mais l'idée est en étude.

Gouvernance de la Continuité d'Activité et de la Gestion de Crise

Les organes qui pilotent le PCA sont le comité opérationnel et de pilotage.

Les PCA sont pris au sérieux par la direction Générale qui est impliquée dans la démarche et comprend la nécessité de traiter la matière. Elle rencontre cependant parfois des difficultés à susciter l'adhésion.

La communication interne se limite quant à elle aux acteurs concernés par le déploiement de la continuité d'activité. Cette communication se fait surtout lors les réunions pour présentation des objectifs, ou sur l'intranet.
La communication externe quant à elle n'est pas anticipée.

Spécificités du secteur Public

Le volet le plus important de la stratégie de continuité d'activité de l'organisation est la continuité opérationnelle, plus particulièrement de l'arrêt d'exploitation des salles de conférence ou leur non accessibilité : cela ferait courir des risques stratégiques et politiques à l'organisation.
L'organisation a déjà connu des incidents, mais pas des situations de crises qui pourraient impliquer les PCA.

Pour notre interlocuteur, les facteurs clés du succès d'un dispositif de continuité d'activité sont les suivants :

- Un positionnement soigné et approprié de la cellule de gestion de crise aux niveaux hiérarchique et organisationnel
- Une communication interne efficace et une bonne préparation de la communication externe, notamment de crise
- Un entrainement et des exercices impliquant le top management et, si possible, en lien avec la Force Publique (Police, Pompiers, RATP…)
- Un système d'astreinte bien établi et encadré