Système de Management de la Continuité d'Activité (SMCA) selon la norme ISO 22301

Guide de mise en place dans une ETI ou une PME

www.clubpca.eu

Une publication du Club de la Continuité d'Activité – CCA
Novembre 2017

Ce document a été produit en novembre 2017, par le groupe de travail ISO 22301 PME ETI du Club de la Continuité d'Activité (CCA)

Remerciements aux participants :

Emmanuel BESLUAU, animateur, Duquesne Group

Jean Luc LEBASCLE, ERMAFLOW

Jean-Paul LEBREC, ALMERYS

Christian MACHOWSKI, Groupe Imprimerie Nationale

Yves MERIAN, Institut pour la Maitrise des Risques (IMdR)

François TÊTE, DEVOTEAM

Nicolas de THORE, ARMATURE Technology

Avant-propos

Cette version a été validée par le Conseil d'Administration du CCA conformément à son règlement intérieur.

Le groupe de travail du CCA ayant participé à la création de ce document ne rassemble que des professionnels traitant de la Continuité d'Activité au quotidien, que ce soit en tant que responsables de la Continuité d'Activité au sein de leur propre entreprise, ou en tant que conseil vis à vis d'entreprises extérieures. Certains d'entre eux sont certifiés « ISO 22301 Lead Implementers ».

Les définitions et les commentaires liés à l'utilisation de certains termes propres à la Continuité d'Activité sont rassemblés dans le document « Lexique structuré de la Continuité d'Activité » accessible sur le site du club à l'adresse « www.clubpca.eu ». Pour en faciliter la compréhension, un résumé des termes les plus souvent utilisés est proposé en annexe.

Ce document n'a pas de valeur juridique mais constitue seulement un recueil de bonnes pratiques entre professionnels à disposition des adhérents du CCA, puis diffusable selon l'accord du Conseil d'Administration.

Table des matières

1. Introduction

La continuité d'activité est une préoccupation inévitable

Des catastrophes récentes, qu'elles soient d'origine naturelle (inondations, cyclones, submersions marines, séismes, …) ou humaine (explosions, attentats, terrorisme, cyber attaques…) montrent à quel point il est important de préparer des réponses pour y faire face.

Ces réponses peuvent prendre différentes formes et votre entreprise a probablement déjà quelques idées de mesures ou actions à mettre en œuvre en cas de nécessité. Peut-être vous êtes vous déjà doté d'un ou plusieurs éléments de Plans de Continuité d'Activités (PCA) et de cellule(s) de crise activables ?

Toutefois, que pensez-vous des divers dispositifs prévus chez vous ? Tiennent-ils compte de votre contexte de risques ? Privilégient-ils correctement ce qui, pour votre métier, est prioritaire ? Proposent-ils des réponses adaptées techniquement et financièrement à vos objectifs ? Vous permettent-ils de décider sous sinistre ? Sont-ils à jour et efficaces ? Vos personnels les connaissent-ils ? Bref, vous inspirent-ils confiance et crédibilité ?

C'est pour pouvoir répondre régulièrement et positivement à ces questions que le Système de Management de la Continuité d'Activité (SMCA) a été mis au point et normalisé par l'ISO 22301. Ce SMCA est cohérent avec d'autres systèmes de management : qualité (9001) – santé et sécurité au travail (45001), - environnement (14001) - sécurité de l'Information (27001).

Objectifs du document

Ce document présente une manière simple et concrète de mise en place d'un SMCA conforme à la norme ISO 22301 et s'adresse en priorité aux PME et aux ETI ayant une complexité limitée (quelques sites – géographie nationale – nombre de centres de profits limité - taille, …) que nous appelons dans ce document « entreprise ».

Il a été réalisé par des praticiens et des experts du CCA (Club de la Continuité d'Activité) dont l'apport d'une expérience de terrain permet de compléter de manière opérationnelle ce qui est indiqué dans la norme ISO 22301.

Il s'adresse principalement aux dirigeants d'entreprises ou d'entités et décrit successivement les actions à réaliser.

Le PCA et le SMCA ? A quoi servent ces outils de la continuité d'activité ?

Définition du PCA selon l'ISO 22301 : un PCA est un ensemble de procédures documentées servant de guides aux entreprises pour répondre, rétablir, reprendre et retrouver un niveau de fonctionnement prédéfini à la suite d'une perturbation.

En préalable et complément, le SMCA est un système de management[1] de votre entreprise, reposant sur un dispositif organisationnel et technique qui, sous l'impulsion et le contrôle de la Direction, permet de mettre en place des réponses face aux diverses situations d'interruptions partielles ou totales, effectives ou potentielles, des activités de l'entreprise. Ces réponses sont adaptées et tiennent compte des priorités et exigences des métiers. Elles aboutissent à des actions suivies et à un Plan de Continuité d'Activité (PCA) opérationnel et vérifié.

Le champ des réponses possibles est large et au choix de la Direction. On trouvera des actions de prévention, de réduction de conséquences, d'atténuation des impacts mais aussi des plans de reprise de divers moyens (IT, locaux, données, transports, usine, etc.) et des dispositifs de gestion de crise.

[1] Dispositif permettant de se fixer des objectifs et de vérifier leur atteinte par des politiques, des processus et procédures, des rôles et responsabilités, des contrôles et évaluations…

2. Lancer votre démarche

EXPOSER VOS INTENTIONS ET LES JUSTIFIER

Objectifs

- Expliquer pourquoi vous lancez cette démarche de Continuité d'Activité et ce qu'elle comporte comme enjeu pour votre métier et votre marché.

Il est important d'indiquer vos priorités d'actions, désigner des responsables impliqués, dédier des moyens et impulser un mouvement en indiquant votre engagement dans une amélioration continue de la situation en matière de continuité

Résultats attendus

Vous publiez une note de la Direction Générale[1] sur la continuité d'activité qui couvre les points suivants (partiel ou global):

- Le périmètre concerné par votre démarche de continuité d'activité (entreprise, activités, sites, entités juridiques, ressources, …) ;
- Les parties intéressées pour lesquelles vous lancez cette démarche (les clients ? le marché en général ? une maison-mère ? des autorités de contrôles ? les employés et vous-même ?) ;
- Les priorités que vous fixez pour cibler la démarche : un service ou site ? une production donnée ? un client particulier ? une exploitation sensible ?
- Le dispositif qui s'en occupera : Responsable du Plan de Continuité d'Activité (RPCA), responsables métiers, DRH, DG, qui seront impliqués dans les actions qui suivent ;
- Le fait que tout ceci sera régulièrement vérifié, qu'il y aura des indicateurs de suivi (contrôle permanent) et une revue régulière par vous-même et la direction.

Comment ?

Vous rédigez une courte note de cadrage et de Politique de Continuité que vous publiez dans votre entreprise.

Cette note de cadrage doit comporter les éléments du contexte interne et externe de l'entreprise et tout ce qui concerne la gestion du projet.

Vous signalez l'attention et l'implication permanente de la Direction Générale sur l'atteinte des objectifs du plan d'action et fixez des revues de direction.

Pour aller plus vite

Une note de Direction indiquant la démarche initialisée, les responsables, l'importance que vous y accordez suffira au début. Un formalisme plus important pourra, éventuellement, être introduit plus tard, notamment pour Intégrer les objectifs du projet de continuité d'activité dans les objectifs individuels des managers impliqués.

[1] Ceci correspond à une note de « politique de continuité d'activité » telle que demandée par la norme 22301

3. Apprécier les risques

A QUELS RISQUES D'INTERRUPTION ETES-VOUS EXPOSÉS ?

Objectifs

- Identifier et connaître les risques d'interruptions possibles de vos activités pour y faire face.

Leur connaissance permet d'identifier et documenter les actions possibles pour réduire les risques et connaitre vos scénarios de menaces les plus impactantes (critiques) face auxquels vous devrez prévoir une réponse.

Résultats attendus

Au terme de cette démarche :

- Vous disposez rapidement d'une vision globale et structurée de vos risques d'interruption, assortie d'un diagnostic partageable ;
- Vous avez la liste des traitements possibles de ces risques avec des indications de priorités.

Vous pourrez ensuite compléter la démarche avec le bilan d'impact sur l'activité (BIA, voir plus loin) pour classer vos activités prioritaires en vue de définir les stratégies de réductions de risques envisageables et les réponses à mettre en place selon les scénarios réalistes déterminés.

Comment ?

L'appréciation et le traitement des risques est un « processus formel et documenté » exigé par la norme.

Le processus comporte quatre étapes que vous allez réaliser en vous focalisant sur les risques qui pourraient interrompre vos activités. Les trois premières étapes correspondent à ce qu'on appelle l'appréciation des risques (identification, analyse et évaluation) et la dernière au traitement des risques.

Il faudra revoir tout cela chaque année afin de prendre en compte toute évolution (produits, processus, type et niveau de ressource, contexte client, demande client, normes et règlementations, site et zone géographique, etc.).

Etape 1 - Identification : constitution d'un portefeuille de risques d'interruption de vos activités

La réflexion sur les risques peut être menée à partir d'un portefeuille des risques existant ou, à défaut, en le créant. Le portefeuille de risques peut être totalement spécifique à l'entreprise, mais il paraît en général préférable (plus simple, plus facile à partager…) de recourir à un portefeuille générique, comme par exemple le portefeuille suivant :

- **6 types de ressources exposées à risques** : bâtiment et infrastructure / informatique / RH / outils et flux de production industriel et de pilotage (ex : centre de commande) /

réseaux (transports, énergie, télécoms, eau, électricité) / prestataires et fournisseurs critiques (logistique, supply chain) ;

- **6 types de risques « majeurs »** : naturels (inondation, séisme, aléa climatique) / pandémie / accident industriel proche (sites SEVESO, transport de matière dangereuse, installation nucléaire …) / cyber menace / mouvements sociaux / terrorisme.

Ces risques sont en partie interdépendants (une inondation peut affecter les installations, le personnel, les fournisseurs et provoquer une coupure électrique …).

Etape 2 - Analyse : élaboration de « scénarios »

En tenant compte de votre contexte, décrivez concrètement le déroulement des événements et la série des effets conduisant à l'interruption d'activité.

Cette analyse permet de trier effectivement ce qui peut se produire et donc déterminer les scénarios de risque ayant les conséquences les plus indésirables sur votre activité et les moyens utilisés.

Etape 3 - Evaluation : détermination du niveau de criticité des risques

Tout risque présente des conséquences nocives 'C' portant notamment sur des moyens qui sont nécessaires à vos activités.

Par ailleurs, l'événement perturbateur possède une vraisemblance plus ou moins importante de se produire.

Il s'agit de positionner C et V dans une matrice de risques (R), avec des jeux de couleurs matérialisant des niveaux de criticité ainsi obtenus (ou gravité : du rouge = le plus grave au vert = le moins grave).

Matrice des risques (R) pour une usine (exemple)

		Vraisemblance (V)			
		Faible	Modérée	Forte	Elevée
Conséquence (C)	Elevée	R7 Inondation usine	R1 Incendie usine R5 coupure électrique usine		
	Forte	R12 Terrorisme stock usine	R6 Fournisseur X critique défaillant R9 pb. gazoduc	R2 accident mat. dangereuse usine	R4 IT salle Usine indisponible
	Modérée	R8 Pandémie	R3 Personnel clé indisponible	R10 Cyber menace IT usine	
	Faible			R11 Mvt social siège	

L'évaluation des risques ci-dessus permet de déterminer, parmi les risques recensés et cotés, ceux qu'il convient de traiter en priorité, en fonction de leur criticité indiquée par la couleur :

Priorités de principe en fonction de la criticité (ou gravité)

A traiter immédiatement
A traiter à court / moyen terme
A traiter moyen terme ou surveiller
Acceptable en l'état

On identifie ainsi les risques qui nécessitent traitement. L'objectif premier est de sortir ceux de la zone rouge dès que possible et de réduire ceux de la zone orange.

Etape 4 – Identification des traitements

Les traitements doivent être proportionnés aux objectifs de continuité. Les « traitements de risques » sont les actions prévues pour mettre sous contrôle les risques ayant un caractère de criticité élevé. En continuité d'activité, le traitement du risque se distingue par :

- Les actions ou mesures préventives, en amont (empêcher la survenance d'un risque) « à froid ». ex : créer une digue, installer les lieux de stockage hors de la zone inondable, acquérir un générateur de courant, fiabiliser les serveurs informatiques, …
- Les actions ou mesures réactives, en aval, à prendre en cas de survenance de la crise (limiter les conséquences en cas de survenance) « à chaud » -ex : déplacer les stocks pour les mettre à l'abri en cas de menace imminente d'inondation, utiliser des pompes de relevage, activer un secours informatique distant, mettre en place du travail (occasionnel) à distance, mobiliser des moyens palliatifs … *mais qu'il faut préparer dès maintenant pour pouvoir le faire quand le risque se réalisera.*

A ce stade, la norme demande d'identifier les traitements qui soient proportionnés aux objectifs de continuité. Il est recommandé d'y indiquer une idée du coût, du délai et de la faisabilité. Ces traitements, ici identifiés, seront développés et décidés dans la partie « stratégie » qui suit, après avoir confronté les risques aux exigences des métiers (partie BIA).

Il est recommandé de dresser un tableau récapitulatif des priorités et des traitements prévus :

Risques	Criticité Ou Gravité	Priorité de traitement	Option de traitement	Actions préventives (prévues à froid)	Actions réactives (prévues suite à événement perturbateur)

Par ailleurs, il faut suivre les risques dont le traitement est moins prioritaire ou qui sont jugés acceptables ou supportables (afin de rester dans le vert ou le jaune).

Ce travail est à refaire chaque année. Cette révision peut se faire très rapidement si rien n'a changé.

Pour aller plus vite

Vous devez au minimum être conscient des 3-4 risques principaux qui pèsent sur votre entreprise et des actions pratiques susceptibles d'être prises pour pouvoir les mettre sous contrôle.

Il n'est pas nécessaire d'aller dans des méthodes sophistiquées et complexes, une rigueur minimale doublée de l'avis des opérationnels de terrain peut suffire. Un formalisme par tableau est utile (« carte des quatre couleurs »).

Il est intéressant de prendre connaissance des données et enseignements disponibles, de la pratique des entreprises proches (confrères, voisins, concurrents …), ainsi que des données disponibles sur les risques auprès des institutionnels (organismes publics[1], professionnels, consulaires).

[1] Notamment : le Dossier Départemental sur les Risques Majeurs (DDRM) : informations essentielles sur les risques naturels et technologiques majeurs du département, consultable gratuitement sur le site de la Préfecture ; le Dossier d'information communal sur les risques majeurs (DICRIM) (informations sur les risques et les mesures / actions), consultable en mairie ; le Plan Communal de Sauvegarde (PCS) pour une commune soumise à un risque ; les plans de prévention de risques majeurs (PPRM), les plans de prévention des risques naturels (PPRN) qui réglementent dans les zones concernées l'utilisation des sols en fonction des risques naturels existants.

4. Faire le Bilan d'Impact sur l'Activité (BIA)

QUELLES SONT VOS ACTIVITES PRIORITAIRES ?

A côté de l'appréciation des risques qui pèsent sur les ressources et l'activité en général de l'entreprise, il faut déterminer et analyser les activités qui présentent des exigences de continuité et reprise. Autrement dit, en cas d'interruption, quelles sont les activités à reprendre vite et dans quel ordre ?

Objectifs

Le BIA (Bilan d'Impact sur l'Activité – Business Impact Analysis) a pour but de déterminer les exigences de continuité et de reprise des activités de production de biens ou de services de l'entreprise[1]. En se focalisant sur vos activités métiers, il s'agit d'évaluer l'impact négatif s'aggravant avec le temps, d'une interruption.

L'analyse permet de déterminer pour chaque activité le délai au-delà duquel l'impact de l'interruption est jugé insupportable, en raison des diverses obligations de l'entreprise.

Pour chaque activité, on déduit alors le DMIA (Délai Maximal d'Interruption Admissible), la PMDT (Perte Maximale de Donnée Tolérable pour son informatique).

Il est aussi requis de déterminer les dépendances et les ressources nécessaires à ces activités, y compris les fournisseurs et autres parties externes.

La détermination des DMIA et des ressources associées servent à définir des priorités pour assurer le maintien et/ou la reprise d'activité dans l'ordre nécessaire et au niveau voulu.

Résultats attendus

A la suite de ce BIA, vous disposez de plusieurs éléments : la liste des activités prioritaires de l'entreprise à maintenir ou redémarrer en cas d'arrêt ; l'explicitation et la justification des DMIA (contractuelles, réglementaires, image, …) ; l'indication des ressources minimales nécessaires pour satisfaire aux exigences de continuité ou reprise.

Cette liste sera discutée et validée en stratégie (étape suivante).

Comment ?

Dans une PME ou ETI cette analyse doit rester simple et pragmatique. Il faut donc, dans l'ordre :

- Identifier sur le périmètre étudié les activités de production de biens et de services en y incluant les flux et les parties intéressées, internes et externes. Un découpage simple doit être utilisé de manière à identifier des lots cohérents d'activités s'appuyant sur des moyens ou ressources utilisés pour ces activités.
- Interviewer les responsables de ces activités pour évaluer avec eux la « montée de douleur » due à une interruption qui dure : pertes financières, détérioration d'image, violation contractuelle ou réglementaire, perte de relations commerciales par défaut de satisfaction des besoins des clients, perte de qualité

[1] Concrètement on analysera aussi les activités « vitales » internes de l'entreprise comme la paie, les déclarations obligatoires, etc.

de service, etc. Pour chaque activité ainsi analysée, on aboutit alors au DMIA, délai au-delà duquel « la douleur est trop forte » ou l'impact est inacceptable. En les classant par DMIA croissant on en déduit les « activités prioritaires [2] » et l'ordre de redémarrage souhaité des activités avec les délais.

- Demander pour ces activités prioritaires quelles sont les exigences et besoins en termes de ressources (humaines, poste de travail, Informatique, bureau, machine, fournisseurs ou partenaire externes etc.) pour un mode de fonctionnement jugé acceptable, qui n'est pas forcément le mode nominal. Les écarts, voire impasses en termes de ressources doivent faire l'objet de propositions d'arbitrages pour bien définir les priorités. Cela sera vu dans le chapitre suivant « stratégie ».

Il convient de récapituler tout ceci dans un ou deux tableaux comme par exemple :

Activité	Financier	Contractuel	Réglementaire	DMIA	RH	IT	PC
Prise d'appel	Impact fort	Impact fort	Sans objet	4 h	5	Call-it	5
Calcul solde usager	Impact moyen	Sans objet	Impact fort	7 h	6	Saldo	4
Planification d'intervention	Impact faible	Impact fort	Sans objet	14h	9	PMW	8
Mise à jour BOM	Impact fort	Impact fort	Sans objet	14h	2	SAP	2

(Notes : « RH » indique le nombre de personnes souhaitables ; « IT » les applications informatiques utilisées ; « PC » le nombre de PC dont il faut disposer. « BOM » désigne un fichier dont l'usine a besoin pour fonctionner dans cet exemple.)

Pour aller plus vite

Cette étape est au cœur de la continuité parce qu'elle désigne les activités prioritaires, celles qui doivent redémarrer au plus vite.

Très souvent par expérience, un directeur d'usine, de PME ou d'ETI peut citer les principales activités prioritaires de son usine ou de tel site. Il faut toutefois ne pas oublier les éventuelles dépendances et vérifier les moyens nécessaires avec les opérationnels du terrain.

Dans tous les cas, il faut avoir déterminé les activités à redémarrer vite et les moyens qu'elles nécessitent en mode minimal acceptable.

On peut toutefois se limiter aux activités qui ont des DMIA allant jusqu'à une semaine, au moins dans une première approche.

Enfin, ne pas oublier *le contexte* de cette analyse. Il est envisagé des situations graves, pouvant aller jusqu'à une interruption forte, voire un sinistre. L'appréciation des risques qui précède nous en a fourni des scénarios. Ceci relativise les choses pour les responsables des activités classées non prioritaires.

[2] Des activités internes telles que la paie, les déclarations obligatoires …sont généralement toujours prioritaires avec des dates butoirs et des modes dégradés possibles.

5. Définir sa stratégie de réponse aux sinistres

QUE FERA-T-ON EN CAS D'INTERRUPTION OU DE MENACE D'INTERRUPTION ?

Maintenant que votre paysage de risques est mieux cerné et que vos activités prioritaires sont identifiées, il va vous falloir formuler une « stratégie de réponse au sinistre ».

Objectifs

L'objectif de la définition d'une stratégie est de se préparer « à tête reposée » pour être prêt à dérouler les opérations le jour du sinistre. Il convient de :

- choisir les actions de traitement / réduction de risque (issues de l'appréciation des risques) que vous décidez de faire ;
- décider des actions de protection, de maintien et/ou reprise des activités prioritaires (activités déterminées lors du BIA avec les niveaux de service acceptable).

Résultats attendus

Il convient de :

- choisir et mener les actions « préventives » pour diminuer les risques d'interruption ;
- décider des activités prioritaires suite au BIA et confirmer les niveaux minimums acceptables et les Délais Maximaux d'Interruption Admissible (DMIA) ;
- définir les exigences en matière de reprise (ou d'arrêt) sur les moyens utilisés et se préparer pour y parvenir ;
- valider les actions de protection et de limitation des délais d'arrêt ;
- prévoir les moyens de secours et la manière de se les procurer, les mettre en œuvre, les exploiter.

Comment ?

Cela consiste, pour une Direction Générale, à décider de certaines orientations, en particulier :

- Appétence au risque : cherchez-vous à réduire vos risques ou acceptez-vous de vivre avec ? Certaines réductions de risques peuvent être pertinentes. Elles se traduisent souvent par des actions de protection, des travaux ou des investissements ;
- Choix de priorités : que décidez-vous pour vos activités prioritaires (issues du BIA) ? Validez-vous les délais maximaux d'interruption admissibles demandés par les responsables (les DMIA) ? Quel niveau de reprise vous paraît jouable ?
- Choix de solutions : avec quels moyens (équipements et machines, informatiques, stocks, etc.), quels effectifs et quelle montée en charge pensez-vous pouvoir y remédier.

- Choix de partenaires : allez-vous vous tourner vers des sous-traitants ou des prestataires en secours ?
- Choix financier : quel budget[3] consacrez-vous à cela ? Quelles priorités ?

Une fois cela décidé, il faut s'occuper des exigences de reprise sur les éléments suivants :

- Comment allez-vous reprendre vos activités ?
- Que préparez-vous comme bureaux de secours ? Où ? En quelle quantité et quel délai ? Peut-on travailler occasionnellement chez soi ou à distance ? Si oui, le préparer.
- Comment préparez-vous le personnel à travailler autrement ou à rester chez soi ? Quelles sont les compétences clés nécessaires ?
- Que préparez-vous pour permettre la reprise de l'informatique (qu'elle soit internalisée ou externalisée) dans des objectifs de temps corrects ?
- Comment protégez-vous vos données ? Et comment sont-elles récupérées sous toutes leurs formes (informatiques ou pas) ?
- Que préparez-vous pour récupérer en règle générale des moyens de production à minima ? Ou préférez-vous tout arrêter « proprement » si le sinistre est trop fort ?
- Qu'exigez-vous des moyens de transport ou de logistique pour vous protéger et faciliter la reprise ?
- Vous avez des fournisseurs dont l'arrêt vous est très préjudiciable : que décidez-vous ? Qu'exigez-vous d'eux comme préparation ?

Ces décisions peuvent vous amener à conclure des contrats avec des sociétés spécialisées ou des accords de réciprocité avec des confrères.

La norme rappelle aussi que l'on doit penser à des points importants comme :

- La priorité de la vie humaine : cela peut dire qu'il vaut mieux arrêter toute activité si le sinistre est trop fort (ex : Cynthia à New-York). Comment arrêter de manière sécurisée ?
- Les actions de réduction des conséquences du sinistre : activer un site de secours c'est bien, mais il faut penser à limiter les dégâts du sinistre sur le site principal. Certaines actions assez simples peuvent s'avérer très utiles : lesquelles ?
- La communication sous sinistre : êtes-vous sûr que vous aurez les moyens de joindre qui il faut, ou d'être joint ? Même dans le désordre causé par le sinistre ? (voir plus loin la gestion de crise).

Une fois ces décisions prises et ces points vérifiés, il reste à documenter les choix faits, réaliser les actions de réductions des risques, prévoir les secours et leur délai d'activiation et formaliser l'ensemble.

[3] Le budget comprend des coûts directs et indirects : projet, assistance, secours informatique et des personnes, solutions spécifiques, implication des collaborateurs, assurance, communication, outils de gestion de la crise et de la continuité d'activité, coût de la crise, maintien des PCA, …

Moyens Exemple :	Sinistre – Evénement grave / redouté	Action	DMIA	Responsable	Remarques	Fiabilisation
IT usine A	Destruction IT	Reprise sur IT usine B	2j	Dir prod	Sur techno 20mm uniquement	So (Sans objet)
IT back-office	Panne ou destruction	Reprise chez prestataire	2j	DSI	+ 20 postes	Onduleur+ générateur
Bureaux siège	Indisponibilité	Repli chez prestataire	2j	Logistique	PC master fixe 15 postes	So
Support prod N2 et N3	Bureaux inaccessibles	Travail distant ou domicile	0,5j	Dir tech	PC portable + VPN	So
Prod usine A	Destruction usine	Mise à l'arrêt de ce qui est sauf	0,5j	Dir prod	Bascule prod sur B en 20mm	So
Stock usine A	Inondation de l'usine A	Déplacement des lots 1 et 2	2j	Logistique	4j de prévenance	Rehausser le stock
Fournisseur(s) critique(s)X	Interruption	Bascule sur fournisseur B	2j	Dir moyens généraux	surcoût	Equilibrer les charges

A chaque fois qu'un prestataire de secours est sollicité, il faut bien évidemment passer un contrat avec lui avant sinistre.

Pour aller plus vite

Reprenez ou réévaluez les activités prioritaires et les délais (DMIA) issus du BIA.

Faites réaliser un tableau comme ci-dessus où vous passez en revue :

- vos moyens les plus sensibles, groupés logiquement ;
- le type d'événement que vous redoutez, générant interruption ou sinistre de votre activité ;
- la réponse que vous envisagez ;
- le Délai Maximal d'Interruption Admissible DMIA ;
- le responsable en charge ;
- des remarques.

Faites circuler ces tableaux parmi vos responsables pour collecter les remarques et les valider.

Mettez en œuvre progressivement les actions de préparation ou de fiabilisation prévues, avec un suivi en revue de direction.

Il faut maintenant faire deux choses :

- décrire et formaliser, par des procédures, ces réponses aux événements perturbateurs (dont sinistres) dans le Plan de Continuité d'Activité (PCA) ;
- définir la cellule de crise qui fera face au sinistre et lancera puis coordonnera l'exécution de ces plans.

6. Documenter le Plan de Continuité d'Activité (PCA)

SUR QUOI S'APPUYER POUR FAIRE FACE A DES EVENEMENTS PERTURBATEURS ? (INTERRUPTION OU MENACE D'INTERRUPTION)

Objectifs

- Disposer d'une documentation qui sert de guide pour le traitement de la crise, de l'interruption, de la reprise ou de la continuité des activités.
- Avoir des procédures (qui fait quoi, quand, comment et où ?) suffisamment détaillées pour bien avancer, mais suffisamment souples pour pouvoir être adaptées au contexte de l'évènement.
- Couvrir tout ce qui a été jugé utile d'activer en cas d'événements perturbateurs générant une interruption d'activité.

Rappel selon l'ISO 22301 : le PCA est un ensemble de procédures documentées servant de guide aux organisations pour répondre, rétablir, reprendre et retrouver un niveau de fonctionnement prédéfini à la suite d'une perturbation.

Commentaires : en fonction de la nature de vos activités, de votre politique de continuité d'activité et / ou de votre culture d'entreprise (appétence aux risques), la décision d'interrompre vos activités peut s'avérer nécessaire et inévitable afin de permettre une reprise d'activité en toute sécurité (sécurité des personnes, sécurité des biens, sécurité des données, …) plus tard. Une procédure de mise à l'arrêt est donc utile.

Résultats attendus

La formalisation de votre PCA doit être adaptée à votre culture et favoriser une traçabilité. Utilisez vos formes de procédures habituelles.

Vous formalisez des documents (procédures, modes opératoires, fiches, …) décrivant ce qu'il faut faire en cas d'activation du PCA : quoi, qui, comment, quand, où ? Ces documents seront déjà connus de ceux qui auraient à les appliquer en cas d'événement perturbateur ou sinistre.

Ces procédures seront utilisées par la cellule de crise et les groupes opérationnels (voir ci-dessous).

Comment ?

Il convient de mettre en œuvre des procédures qui doivent globalement contenir :

- Les rôles et responsabilités (individu responsable, acteur concerné) ;
- La manière de se coordonner et de communiquer (entre personnes et avec la cellule de crise) ;
- La manière de déclencher tel ou tel secours (qui contacter ? quoi dire ? quel N° de contrat ?) ;

- Des actions de protection (des personnels, biens, etc.) et de limitation des dégâts ;
- Une coordination opérationnelle avec les clients les plus impactés ;
- La manière de planifier et effectuer la reprise des activités prioritaires ;
- Des indications techniques nécessaires.

Ces procédures font ou peuvent faire référence à des modes opératoires contenant en particulier des éléments plus précis tels que : schémas, modèles, images fixes ou vidéos, des adresses de sites internet, etc.

On couvrira, par un PCA documenté, par exemple, les réponses suivantes :

- le recours à un secours informatique ;
- le travail occasionnel à distance ;
- l'usage de PC portables avec accès VPN (accès sécurisé à distance) ;
- le recours à des bureaux alternatifs ;
- la mise à l'arrêt d'une exploitation ;
- la recherche et restauration de sauvegardes informatiques ;
- le travail en mode dégradé papier ou PC ;
- l'activation de moyens informatiques de développement pour faire de la production.

Et plus généralement tout ce qu'il est jugé bon de décrire pour guider les actions de manière suffisante en cas d'événement perturbateur (potentiel ou avéré) ou sinistre.

D'un point de vue ergonomie, un PCA peut être partiel ou global. S'il est global, il peut être décliné et s'appuyer sur des PCA intermédiaires par entité / métier / site / bâtiment etc.

Pour aller plus vite

Si vous ne disposez pas de ces procédures, vous pouvez commencer par utiliser le déroulement écrit de test ou d'exercice (voir plus loin) que vous suivez régulièrement. Vous les complétez des éléments écrits nécessaires pour guider le lecteur dans la réalisation des opérations.

Vous pouvez également vous appuyer sur des outils et résultats issus de démarches préalablement engagées sur vos processus de travail (comme ISO 9000 et 14000, Qualité totale, Business Process Management, Lean, …) sachant tout de même qu'on se concentre sur le minimum nécessaire.

Ces procédures doivent être simples et pragmatiques car elles doivent pouvoir être utilisées par d'autres que les « sachants », qui eux, peuvent être absents ou empêchés au moment de l'interruption ou du sinistre.

7. Préparer la cellule de crise[4]

COMMENT DECIDER ET PILOTER SOUS CRISE ?

Objectifs

Dans le cas d'un incident perturbateur majeur ou d'un sinistre, en situation d'incertitude ou d'urgence dans laquelle le processus de décision normal n'est plus adapté, la Cellule de Crise Décisionnelle (CCD) est la seule instance de l'entreprise qui doit avoir la capacité de décider.

Cette Cellule de Crise Décisionnelle (CCD) a un rôle de pilotage et de coordination : piloter la gestion de crise, assurer la communication de crise (entrante et sortante), arbitrer les décisions importantes, donner les instructions aux équipes opérationnelles et fonctionnelles. C'est « la tour de contrôle » !

Selon l'entreprise et l'ampleur de la crise, une ou plusieurs Cellules de Crise Opérationnelles (CCO) peuvent être mises en place en aval de la CCD pour mobiliser les services et les experts sur le terrain.

Résultats attendus

Disposer d'une CCD capable d'assurer :

- La sécurité :
  - Des personnes (la première priorité des membres de la cellule de crise) ;
  - Des biens, de l'écosystème (parties intéressées) et de l'environnement.
- La continuité d'activité :
  - Assurer autant que possible les activités prioritaires au moins en mode dégradé ;
  - Arbitrer le cas échéant entre la suspension et la continuité d'activité ;
  - Piloter la reprise d'activité et le retour à une situation normale.
- La communication (entrante et sortante) :
  - Interne (personnel, IRP, CHSCT, métiers, …) ;
  - Externe (médias, autorités, partenaires, …) ;
  - … En veillant à la réputation de l'entreprise.
- La traçabilité :
  - Des évènements ;
  - De la conduite de crise (décisions, engagements financiers,…) ;
  - Des retours d'expérience (coûts, incidents, impacts, dépendances, points d'inefficacité).

[4] Cette partie est assez peu détaillée dans la norme ISO 22301. Nous avons décidé de l'enrichir de l'expérience des membres du CCA.

Missions

Les missions de la Cellule de Crise Décisionnelle (CCD) sont de :

- Collecter l'information (interne et externe, y compris l'évolution de la situation) ;
- Analyser l'événement et ses impacts :
  - Apprécier la nature et l'ampleur de l'événement ;
  - Anticiper ses évolutions possibles (dégradation à attendre ou non) ;
  - Intégrer les aspects humains en premier, matériels, financiers, engagements ;
  - Proposer les actions en réponse à la crise.
- Prendre des décisions et arbitrages de façon rationnelle et objective :
  - Activation du PCA global ou de parties spécifiques ;
  - Décision d'actions autres, spécifiquement liées à la situation (par exemple : renvoi de personnels chez eux, arrêt sécurisé, reprises hors PCA, recours à des aides) ;
  - Maîtrise de la sécurité, respect des lois et règlements, défense des droits de l'entreprise ;
  - Coordination centrale de l'ensemble des actions et acteurs.
- Communiquer de manière maîtrisée en interne, en externe et vers les parties prenantes. Rester joignable, en particulier pour les autorités et les instances prioritaires.
- Formaliser les évènements et les prises de décisions (opposable juridiquement et envers les assurances) ;
- Faire le retour d'expérience de crise (REX ou RETEX) à chaud (le plus rapidement possible) et à froid. Ensuite, rédiger un bilan et un plan de progrès validés par la Direction pour engager les actions d'amélioration.

Composition

La CCD est composée, au minimum, des membres suivants :

- Un représentant de la Direction (bien souvent Directeur de site ou de l'entreprise) qui peut au besoin s'entourer de responsables tels que DRH, juridique, communication ;
- Un ou plusieurs responsables en charge des moyens sinistrés et des moyens de secours (ceux-ci dépendant du sinistre, mais en général : informatique, usine, bureaux, …) ;
- Le RPCA en tant qu'expert du sujet (dans une PME cela peut être l'un des précédents) ;
- Un responsable ayant la vision des clients et parties intéressées ainsi que des divers engagements pris de production ou exploitation.

Il est de plus nécessaire d'avoir en cellule de crise des membres qui vont faciliter l'intendance

- pour la collecte des événements et la traçabilité : un « scribe » ou secrétaire (tenant une main courante) ;
- pour le suivi du temps et le respect des délais : un « time keeper » (surveillant le temps qui passe).

Pour être efficace, la CCD doit se composer de 3 à 7 membres maximum et chacun doit disposer de suppléants.

La CCD peut s'appuyer sur des Cellules de Crise Opérationnelles (CCO) composées d'opérationnels de terrain, d'experts métiers ou techniques, d'experts en communication, RH, Logistique et sécurité, SI, …

Fonctionnement et moyens

La CCD doit se constituer rapidement et efficacement en cas d'alerte (avoir un dispositif d'alerte et d'astreinte). Les membres de la CCD doivent être capables de réagir promptement à tout évènement et de prendre les bonnes décisions pour son personnel et l'activité de l'entreprise et de ses clients. Il convient d'apporter une attention particulière au facteur humain pour la conduite de la gestion de crise.

La cellule de crise et ses membres doivent être dotés :

- d'annuaires de crise (intervenants indispensables, contacts utiles tenus à jour) ;
- d'un plan de gestion de crise (document qui décrit son organisation, ses missions et son fonctionnement à base de pense-bêtes) incluant une salle identifiée et équipée et les outils de liaison appropriés (téléphonie mobile, Intranet, messagerie instantanée, alertes sonores et visuelles, micros…) ;
- du PCA (servant de guide) ou de parties de PCA appropriées.

Pour aller plus vite

Notez sur une feuille de papier[5] (ou au format carte de crédit, ou sur vos outils numériques mobiles) le nom des personnels et responsables qui seraient nécessaires en cas de perturbation, avec les N° de téléphones (non abrégés) et adresses e-mail. Conservez-la sur vous.

Collectez la documentation utile en cas de crise (les BIA et modes dégradés, le PCA et procédures de reprise, les contacts des secours et moyens d'activation, etc.).

Identifiez un bureau ou une salle de crise, aisée d'accès et à l'abri des événements perturbateurs ; mettez-y la documentation utile (avec copie accessible en ligne).

Sensibilisez à tout cela les responsables concernés et demandez-leur de faire comme vous.

[5] Dans le respect des directives CNIL et de la future Directive européenne RGDP Réglementation Générale des Données Personnelles qui protège les données privatives des personnes physiques (25 mai 2018)

8. Organiser des exercices et des tests

COMMENT S'ASSURER REGULIEREMENT QUE CES DISPOSITIFS FONCTIONNENT ?

Le PCA existe, il va falloir maintenant le mettre à l'épreuve de la réalité par des tests et exercices représentatifs.

Objectifs

- Vérifier que les dispositifs prévus sont réalisables et adaptés (tests et exercices). En effet, par expérience, un PCA insuffisamment testé présente tous les risques de ne pas fonctionner en cas de besoin. Les investissements réalisés précédemment ne servent alors à rien ;
- Evaluer la capacité de l'entreprise à gérer une crise et la reprise de ses activités après sinistre ;
- Concrétiser l'intérêt du PCA auprès des collaborateurs participants par son utilisation en situation prédéfinie ;
- Gagner en visibilité et légitimité auprès des parties prenantes ;
- Détecter des améliorations possibles ;
- Capitaliser sur les solutions mises en œuvre (exercices).

Résultat illustré par un exemple

Etapes d'exécution d'un exercice de validation de tout ou partie d'un PCA selon un scénario prédéfini :

Préparation	Déroulement	Retour d'expérience
• Définir les objectifs • Qualifier le périmètre • Planifier les tests / l'exercice • Communiquer sur l'exercice • Réaliser des tests techniques • Définir les tâches à réaliser • Fixer le timing	• Mettre en place le pilotage de l'exercice : suivi, contrôle, communication, observation • Recueillir des preuves et des résultats de l'exercice	• Recueillir les informations des participants lors d'un débriefing à chaud • Faire un débriefing à froid en présentant le compte rendu de l'exercice • Diffuser les résultats et mener les plans d'action

Comment ?

Il faut distinguer deux approches :

- Les tests qui vérifient des dispositifs techniques (disponibilité des ressources, restauration des données, disponibilité des applications, re-routage de la téléphonie ou du réseau, redémarrage de telle machine,…) ;
- Les exercices qui entrainent les collaborateurs mis dans une situation proche de la crise à réaliser ce qu'est la continuité d'activité en s'appuyant sur l'organisation de crise, la documentation et les outils correspondants.

Un test ou un exercice selon la norme doit :

- Correspondre au périmètre et aux objectifs de reprise ;
- Avoir un objectif précis et déterminé (un niveau de service à atteindre dans tel délai) ;
- Correspondre à des scénarios réalistes (vus plus haut) ;
- Etre varié afin que, tous cumulés au fil du temps, cela valide les dispositifs en place ;
- Ne pas risquer de causer des interruptions non prévues (effets collatéraux indésirables) ;
- Produire des résultats, des rapports, des actions d'améliorations à faire, qui soient pilotées ;
- Etre fait régulièrement et lors de changements dans l'entreprise.

On peut aussi recommander :

- Une implication de la Direction Générale et des parties prenantes ;
- Une préparation limitée ;
- Une croissance progressive dans la difficulté des exercices ;
- Une formalisation systématique (main courante) des actions, évènements, décisions, réactions observés et mis en œuvre

Pour aller plus vite

Dès que vous disposez d'éléments précis et documentés (gestion de crise, PCA, contrat de secours, …) mettez-les à l'épreuve en organisant :

- Des exercices en salle sur documents pour les évaluer ;
- Des exercices sur site en réel, par exemple lors de périodes de maintenance ou d'inventaire, de sous activité, de période de test de sûreté / sécurité ;
- Des tests techniques de reprise de machines, de restauration de sauvegardes, … ;
- Des simulations de sinistre, sans prise de risques ;
- Des exercices de lancement de cellule de crise, avec mobilisation des acteurs concernés.

Faites préparer des plans de déroulement des tests et faites un retour d'expérience avec des plans d'actions et d'amélioration. Tout cela contribue à valider la démarche et à rester concret.

9. Sensibiliser / Former

QUI SENSIBILISER OU FORMER ET COMMENT ?

Objectifs

- S'assurer que l'ensemble de la direction et du personnel a intégré les principes de la continuité d'activité en cas de sinistre ou d'événement perturbateur majeur, les moyens et l'organisation mis en œuvre pour y répondre ;
- Former de manière plus approfondie les acteurs de la direction et du personnel ayant un rôle opérationnel réel pour assurer la continuité d'activité de l'entreprise.

Résultats attendus

Il s'agit de sensibiliser et/ou former les personnels au travail en situation de crise, il est donc important, de s'assurer auprès de chacun :

- Des bons niveaux de compréhension du sujet de la continuité et de la gestion de crise ;
- De l'engagement et de la maitrise de son propre rôle ;
- De la connaissance des outils à utiliser.

Chacun doit savoir le rôle qu'il peut avoir à jouer en cas d'interruption ou de sinistre.

Comment ?

Tout le monde de l'entreprise est sensibilisé, les acteurs de la reprise ont en plus une formation spécifique.

La sensibilisation

Tout le personnel doit recevoir environ 1h30 à 2 heures de sensibilisation.

Les objectifs sont les suivants :

- Comprendre la différence entre incident courant et événement majeur impactant l'entreprise ;
- Comprendre les notions menace - risque – scénario de risque – plan de continuité d'activité – solutions de secours – gestion de crise ;
- Appréhender les solutions et outils de continuité en place, l'organisation et les réflexes à avoir en cas de crise, connaître l'expérience déjà vécue par l'entreprise et son retour d'expérience, identifier les règles à suivre en cas de crise, etc.

La formation

Selon l'organisation et l'ampleur du sinistre, une Cellule de Crise Décisionnelle (CCD) et plusieurs Cellules de Crise Opérationnelles (CCO) et de supports techniques peuvent être mises en place de façon coordonnée. Les personnes de ces cellules ayant un rôle plus actif, en particulier par la mise en œuvre ou l'utilisation de solutions de continuité devront, quant à elles, être formées annuellement.

Cette formation peut se dérouler de plusieurs manières :

- Sous forme d'atelier par service sur un thème particulier (continuité IT, continuité du service X, continuité du bâtiment Y – etc.) ;
- Ou de manière plus collective liée à un scénario de sinistre (pandémie – attentat – intempéries – manifestation dans la zone - inondation – etc.).

Dans tous les cas, cette formation doit permettre à chacun :

- De situer son rôle dans les opérations des Cellules de Crise (Décisionnelles ou Opérationnelles) et de support ;
- D'identifier et de prendre connaissance sur site en réel des solutions et environnements de continuité à utiliser ;
- D'appréhender l'organisation, les procédures et modes opératoires à utiliser ;
- De se familiariser avec les outils de crise et de continuité (ex : pocket mémo format carte de crédit) sur lesquels s'appuyer, (annuaire de crise, plan d'accès, téléphone de crise, règles à suivre, conditions de travail en situation de crise, etc.) ;
- De se préparer à réaliser des exercices ;
- D'identifier quelle pourrait être l'évolution de ses propres fonctions en cas d'indisponibilité de l'un ou de l'autre de ses collègues.

Pour aller plus vite

Parmi les premiers éléments à maitriser, il faut noter :

- Le « pocket mémo » rappelant les coordonnées de collaborateurs utiles en crise et les outils d'intendance de crise ;
- Les documents de procédures et modes opératoires (comment y accéder et les utiliser) ;
- Des mails et SMS d'alertes pré-formatés pouvant être envoyés simultanément à de multiples destinataires ;
- Le fait que les personnes mobilisables en cas de crise sachent effectivement quoi faire et où aller ;
- Les outils de mobilité intégrant PC portables, smartphones, documents, applications, listes, liens vers sites Internet.

10. Faire fonctionner votre SMCA

COMMENT OBTENIR LA MAITRISE ET L'EFFICACITE DE SON SMCA ?

Objectif

- Etre en mesure de piloter le système de management, au niveau Direction, afin d'obtenir les résultats attendus en matière de continuité.

Sous votre initiative et dans le cadre de votre politique de continuité d'activité (chapitre 1), diverses actions ont été lancées dans l'entreprise pour assurer la Continuité d'Activité.

Il faut donc mettre en place ce qui est nécessaire pour voir rapidement où l'on en est et ce qu'il faut éventuellement corriger.

Résultats

La Direction Générale doit disposer, c'est une exigence de la norme, de moyens d'information :

- Des indicateurs ciblés mis en place, mesurés et présentés régulièrement par le RPCA ;
- Des revues diverses et leurs comptes rendus ;
- Des retours sur événements (résultats des tests et exercices, pannes ou interruptions vécues, etc.) ;
- Des rapports d'audits internes.

Il est nécessaire que la Direction Générale aborde les points ci-dessus au moins une fois par an dans le cadre d'une réunion de direction sur ce sujet de la « continuité d'activité ». Lors de ces revues, elle peut éventuellement décider d'actions de réorientation et correction.

Comment ?

Dans une PME ou une ETI, il faut rester simple et réaliste sur ces aspects.

Mettez en place très vite quelques indicateurs correspondants à vos craintes : taux de réalisation des BIA ? Taux de succès des tests ? Nombre de risques connus et traités ? % d'exercices réalisés ? % ou nombre de personnes sensibilisées ? % ou nombre de personnes formées ?

Faites réaliser un audit interne simple à base de questions (pas plus de 30) suivant les chapitres qui précèdent. Dans une ETI en particulier, mobilisez le contrôle interne et articulez le SMCA en lien avec la direction / le management des risques.

Réservez dans vos réunions de Direction un point d'ordre du jour sur la Continuité d'Activité où vous passez en revue les indicateurs, les événements de type interruption et les résultats d'audit. Eventuellement « corrigez le tir ».

Pour aller plus vite

Il vous faut très vite pouvoir suivre ce que donnent les actions lancées.

Exigez d'être régulièrement informé avec des indicateurs simples.

Décidez à minima un audit interne rapide.

Réservez dans vos réunions de Direction un point d'ordre du jour sur la Continuité d'Activité où vous passez en revue les événements d'interruption, les indicateurs et résultats d'audit.

11. Conclusion

La continuité d'activité ne s'improvise pas !

Le bâtiment est inondé, vos 200 collaborateurs sont sur le parking…

Savez-vous quelle activité il faut traiter en premier ? Et ensuite ?

Qui doit rester ? Pour travailler où ? Qui doit rentrer chez lui ? Et dans quelles conditions ?

Qu'est devenu le stock prêt à livrer ? Où mettre la livraison qui arrive demain ?

De plus ce sinistre n'était-il pas prévisible ? N'y avait-il pas quelques travaux réalisables préalablement qui en auraient limité les conséquences ?

Une préparation est possible mais également indispensable.

Connaître votre exposition aux risques d'interruption, voire de sinistre et de tout autre type d'arrêt est possible. Traiter les plus critiques doit être réalisable.

Identifier ce qui doit redémarrer vite sur votre site ou sur un autre et quels moyens minimaux il faut pour cela est judicieux.

Planifier des reprises avec des moyens de secours (informatiques et autres) adaptés selon votre budget reste très utile en cas de sinistre.

Identifier vos activités prioritaires pour mettre en place un PCA approprié, piloté par une cellule de crise compétente, est le préalable à la mise en œuvre d'un Système de Management de la Continuité d'Activité (SMCA) dans votre entreprise.

Ce SMCA vous permettra de fixer les objectifs de continuité adaptés à vos besoins, de les atteindre progressivement en fonction de vos contraintes et priorités définies, de faire valoir à qui de droit en permanence, la mise sous contrôle des opérations de continuité en cas d'événement majeur.

***

Annexe 1 - Foire aux questions

Nous recensons ici de nombreuses questions que se posent régulièrement les dirigeants réfléchissant à mettre en œuvre un système de management de la continuité au sein de leur entreprise.

Trois thèmes de questions / réponses sont proposées :

- A : GENERAL – intérêt d'une approche PCA – obligations - …
- B : ETAPES de mise en œuvre – politique – types de risques - BIA - types de solution - …
- C : NORME – certification – audit – assurances - …

GENERAL – intérêt d'un PCA - pourquoi ?…

Ref	N°	Question / Objection	Réponse
A	1	Pourquoi dois-je me préoccuper du sujet de la continuité ?	C'est un sujet d'actualité. De nombreux services font preuve de pannes longues et handicapantes. Cela inquiète beaucoup de monde. Nous sommes dans un monde d'interdépendances. Si un de vos fournisseurs ne pouvait pas assurer le service attendu même en cas de sinistre à son niveau, qu'en penseriez-vous ? Et vous, en tant que fournisseur, que pensez-vous de la réaction de vos clients ? De plus, pour se convaincre de l'importance du sujet, il suffit de réfléchir aux conséquences sur votre activité si elle venait à être interrompue par un événement redouté.
A	2	Il va me falloir des consultants, cela revient cher	Le coût des consultants est à rapprocher des coûts d'une rupture d'activité. Il est possible d'avoir une approche à minima adaptée à votre taille. Les consultants peuvent intervenir de manière limitée, vous apporter un savoir-faire que vous utiliserez pour mettre vous-même en place le dispositif le plus adapté.
A	3	J'ai assez à faire avec la Qualité (et la Sécurité) pour ne pas avoir à me préoccuper de continuité !	Les systèmes de management de ces disciplines (Qualité – Sécurité – Continuité) sont assez similaires ; Si vous avez déjà effectué une démarche sur les 2 premiers, le surcoût pour le domaine de la continuité peut être réduit.

A	4	Il va me falloir former du monde ; j'ai d'autres priorités que ce sujet	La formation en question peut être assez légère et immédiatement bénéfique. Ce guide est une première étape de sensibilisation au sujet de la continuité pour vos collaborateurs.
Ref	**N°**	**Question / Objection**	**Réponse**
A	5	Rien ne peut remplacer la vigilance du PDG et la compétence de ses adjoints	Tout à fait exact. Mais pensez-vous que ce soit suffisant ? Toute l'organisation ne peut pas reposer que sur quelques-uns.
A	6	Nous avons un PCA depuis cinq ans, cela me suffit	Etes-vous certain qu'il est à jour et opérationnel ? De quand date le dernier test ? le dernier audit ? Un PCA est un document et un outil vivant. Il doit être actualisé régulièrement.
A	7	Avant de prévoir ce qui n'arrive jamais, je préfère penser aux ennuis qui m'arrivent souvent	L'un n'exclut pas l'autre. De plus, « le risque zéro n'existe pas ». En cas de sinistre, il faut avoir prévu un minimum de réponse. Par ailleurs, les interruptions « fréquentes » peuvent être anticipées et supprimées par une analyse de risque …
A	8	Pourquoi passer autant de temps à faire un Plan qui risque de ne jamais servir ?	Il n'est pas nécessaire d'y passer beaucoup de temps. Un minimum est cependant souhaitable. Ce plan vous prépare à réagir aux interruptions, et d'abord à les identifier en commençant justement par les plus probables.
A	9	Mon concurrent avait un PCA ; il a pourtant été inondé et a perdu son stock, alors ?	Le PCA permet de limiter d'une part les risques que vous maîtrisez et d'autre part les impacts des catastrophes. On peut déduire de cet événement plusieurs hypothèses : a) Risque de perte des stocks accepté explicitement par la direction ; b) Appréciation insuffisante (l'analyse de risques de votre concurrent était imparfaite, risque d'inondation non pris en compte, mesures / actions de sauvegarde des stocks non prévues, insuffisantes ; c) PCA méconnu ou mal appliqué ou obsolète ; d) Circonstances trop éloignées des scénarios gérables par votre concurrent. Un PCA n'empêchera pas l'inondation de se produire mais peut éviter de laisser détruire des biens, si c'est possible et permettre de s'en sortir plus vite que sans Plan.

A	10	C'est à mon fournisseur que j'aimerais demander d'avoir un PCA !	Pourquoi pas ? Cela peut s'ajouter aux clauses contractuelles. Au même titre que vos clients peuvent vous demander si vous avez un PCA et un SMCA certifié, vous devez faire de même avec vos fournisseurs les plus essentiels. Cependant, « avoir un PCA » ne suffit pas ; encore faut-il qu'il soit approprié et testé. Suggestion : demandez le rapport des tests.
Ref	**N°**	**Question / Objection**	**Réponse**
A	11	Je ne vois pas de retour sur investissement d'un tel projet PCA	Le retour sur investissement d'un PCA se justifie d'une part dans l'assurance que vous donnez à vos clients et d'autre part pour vous-même en cas de sinistre, par une limitation de vos pertes et une reprise plus rapide de votre activité.
A	12	Je n'ai pas le temps de faire un PCA ou SMCA	Ce n'est pas forcément long et complexe à entreprendre et vous pouvez le déléguer à l'un de vos cadres.
A	13	Quand un client me demande si j'ai un PCA je lui réponds toujours que j'en ai un même si ce n'est pas vrai car il faut bien le rassurer. De toute façon on n'a jamais eu de problème majeur	Et si demain vous avez un audit ou un sinistre, vous perdrez votre client car vous aurez menti lors de ses interrogations. Ce type de réponse n'est plus tenable en 2017. Il n'y a que deux types d'entreprises : celles qui sont en situation de crise et celles qui le seront.
A	14	J'ai une bonne assurance donc je n'ai pas besoin de PCA et encore moins d'une certification	Vous pensez sans doute que c'est l'assurance qui va vous permettre de redémarrer votre activité et surtout, ainsi, vous ne perdrez pas de temps dans sa reprise ? Une assurance « indemnise » au bout de… un certain temps, ce n'est pas pour autant qu'elle permet la continuité des activités. En attendant, vos clients sont allés voir ailleurs…

A	15	Si je mets en place un PCA, Il va falloir le mettre à jour. Je n'ai pas envie de me rajouter une contrainte récurrente	Tout cela s'organise et peut être limité grâce à une bonne organisation mise en place dès le départ.
A	16	Ce qui m'intéresse, ce n'est pas d'avoir un PCA mais de sécuriser ma production et mes flux	Ceci n'est pas antinomique, bien au contraire. De plus il serait bien de sécuriser également vos partenaires, clients et fournisseurs en les assurant de votre capacité à offrir le service attendu même en cas de sinistre.

ETAPES de mise en œuvre – types de solution – BIA – méthode, etc…

Ref	N°	Question / Objection	Réponse
B	1	On me dit qu'il faut une politique de continuité, je n'en vois pas l'intérêt	Vous avez certainement votre politique en tête, il convient d'en exprimer par écrit les conséquences pour votre entreprise. L'intérêt d'avoir une politique formalisée de continuité d'activité est de pouvoir en faire mention dans vos réponses aux appels d'offres de vos clients et de vous valoriser par rapport à la concurrence. Une politique formalisée permet également à vos collaborateurs de comprendre les enjeux et d'être convaincus qu'il ne s' « agit pas d'une énième déclaration commerciale ».
B	2	Je sais bien quelles sont mes activités prioritaires, cela me suffit amplement	C'est un bon point de départ. Mais en votre absence, êtes-vous sûr que cela sera suffisant ? Les opérationnels ont-ils la même appréciation que vous ? Ce constat est-il partagé par vos collaborateurs et avez-vous mis en place les moyens de limiter les impacts d'une crise sur ces activités.
B	3	Je n'ai pas envie de faire connaître mes risques à tout le monde	Vos analyses de risques peuvent rester confidentielles. L'intéressant n'est pas de faire connaitre vos risques mais d'assurer « à tout le monde » que vous maîtrisez votre activité et que vous assurerez la qualité de service attendue.
B	4	Je veux pouvoir décider seul des risques que j'accepte de courir	La norme ne dit pas autre chose, mais l'avis d'autres personnes ne peut-il pas vous être bénéfique ? Effectivement, vous pouvez décider seul mais êtes-vous prêt à faire courir les mêmes risques à vos parties prenantes (clients par ex).
B	5	Quel est l'écueil majeur dans cette démarche SMCA – 22301 ?	En se lançant dans cette démarche, les risques majeurs pour une PME / ETI sont d'une part de vouloir couvrir « tous » les risques d'indisponibilité de l'entreprise et de ne pas y arriver, d'autre part d'effectuer cette démarche sous la pression ponctuelle d'une autorité (audit interne / externe) et de ne pas maintenir dans le temps le SMCA. Enfin, le risque est de confier ce sujet à une personne ou trop technique ou qui n'a pas la culture « système de management » suffisante.
B	6	Mes moyens de reprise ne regardent que moi ; Ils relèvent du domaine confidentiel	Il est effectivement possible de garder cela confidentiel. L'auditeur sera soumis à confidentialité si vous le voulez ainsi que les détails de l'audit, bien évidemment. Toutefois, il est valorisant de pouvoir indiquer à vos clients que vous avez un PCA et un SMCA, sans forcément entrer dans les détails.
Ref	**N°**	**Question / Objection**	**Réponse**
B	7	Il ne peut rien m'arriver car toutes mes données sont chez xxx qui a un PCA	Avez-vous vérifié ce PCA ? N'y a-t-il que vos données comme biens sensibles présentant un enjeu …? Et vos activités critiques ? Demandez-donc à xxx son rapport de test de PCA !
B	8	En cas de sinistre, je peux travailler de chez moi	Oui bien sûr. Et vos employés / collaborateurs ? Cela peut aussi faire partie de votre PCA.
B	9	Un sinistre ne peut pas m'arriver parce que mon informatique est sécurisée à l'extérieur	Un PCA ne concerne pas seulement l'informatique. Il concerne également l'ensemble du fonctionnement de votre entreprise et tous vos moyens (bureaux, machines, stock, etc.). De plus, l'extérieur dont vous parlez est exposé lui aussi à des risques.
B	10	J'ai un back-up de ma chaine de production dans le bâtiment d'à côté donc je n'ai pas de souci	Et si vous subissez un sinistre de zone, comment faites-vous ? Un événement redouté (sinistre ?) pourrait toucher vos 2 chaines. Seule, votre analyse de risques et votre cartographie permettront de confirmer (ou pas) votre affirmation.
B	11	Il va me falloir faire des tests ; or ma production ne peut pas s'arrêter	Il faut alors aménager les tests pour qu'ils gardent une valeur probante et minimisent vos interruptions. Dans un premier temps, vous pouvez commencer par des tests sur table sans arrêter votre processus de production.

NORME – Certification – audit – assurances - …

Ref	N°	Question / Objection	Réponse
C	1	J'entends dire que les normes paralysent l'innovation	L'innovation fait-elle partie de vos processus critiques ? Les normes de management vous proposent une approche qui vous laisse libre de vos choix sur les aspects techniques où réside votre innovation.
C	2	Mon souci ce sont les parts de marché, pas les normes	Répondre aux normes peut justement vous apporter de nouvelles parts de marchés car cette demande figure de plus en plus dans les appels d'offres. De plus, le respect de normes de management peut rassurer vos clients potentiels.
C	3	Aucune norme ne doit pouvoir décider à ma place	Tout à fait d'accord. La norme ne dit pas le contraire. Avec ou sans norme, vous devez prendre des décisions, en particulier en matière de continuité d'activité.
Ref	**N°**	**Question / Objection**	**Réponse**
C	4	Qu'apporte la norme ISO 22301 pour mon entreprise ?	La norme ISO 22301 apporte une démarche permettant d'identifier les points nécessaires à la mise sous contrôle permanente d'un Système de Management de la Continuité d'Activité (SMCA). Une fois en place, ce SMCA ISO 22301 devient une valeur ajoutée reconnue par le milieu professionnel.
C	5	Quelle est la première étape à prendre en compte pour un SMCA sous contrôle, cohérent avec l'ISO 22301	Reportez-vous au début de ce document § « lancez votre démarche ». Il est demandé un engagement de la direction vers une amélioration continue de la capacité de continuité d'activité de l'entreprise.
C	6	Pourquoi me faire certifier ?	Pour démontrer une capacité technique et organisationnelle, validée par un tiers et maintenue et améliorée dans la durée.
C	7	Est-ce que l'Etat ou autre m'oblige à avoir un PCA et à me certifier ?	Cela dépend de votre activité. Certains appels d'offre peuvent vous y obliger pour soumissionner.
C	8	Je ne crois pas qu'une certification remplace la vraie compétence	Tout à fait exact. La certification peut en partie confirmer la compétence, mais l'absence de compétence empêche la certification.
C	9	On me parle de système de management certifié… Qu'est-ce que cela signifie ?	Il ne s'agit pas au sens strict de votre entreprise. C'est son système de management qui est certifié et votre organisation permet d'avoir des réponses appropriées aux sinistres. En complément : c'est d'ailleurs l'intérêt de cette certification. Une fois réalisée, elle permet de garantir les réponses que vous apportez aux risques identifiés. Il en va de même pour d'autres systèmes de management : la qualité (SMQ) ou la sécurité de l'information (SMSI).

Ref	N°	Question / Objection	Réponse
C	10	Si on commence à mettre le doigt dans l'engrenage de la certification, on devient soumis à plein de contraintes coûteuses pour la conserver : non merci !	Les contraintes sont nécessaires pour éviter la détérioration de vos plans et réponses dans la durée. Vous le savez, sans surveillance, tout finit par perdre en efficacité. Ne voyez pas cela comme une contrainte mais évaluez ce que cela peut vous apporter, vous rapporter et vous éviter.
C	11	Je suis trop dépendant de mes fournisseurs pour qu'une certification ait du sens !	Au titre de votre propre système de management, vous pouvez leur demander d'être audités, et faire pression sur eux pour prouver la réalité d'un management de la continuité. Ils sont parties prenantes et vous devez donc les associer à votre démarche. De plus, mettre en place un PCA et un dispositif de certification vont vous permettre de réfléchir sur le moyen de limiter votre dépendance et d'assurer la qualité de service attendue par vos clients en connaissance de cause. Bref, vous reprenez la maitrise de votre politique d'achats.
Ref	**N°**	**Question / Objection**	**Réponse**
C	12	Une certification ça ne sert à rien. Ce n'est qu'un bout de papier qui n'apporte rien à ma production	La certification apporte avant tout la preuve d'un cadre vérifié par un tiers, ainsi que l'assurance de qualité de service à vos clients.
C	13	Je suis déjà audité par mes clients plusieurs fois par an : cela me coûte et doit suffire !	Il est possible que cela change : votre certification ISO devrait suffire aux auditeurs clients qui limitent alors leurs investigations
C	14	Il va falloir subir des audits répétés à mes frais : combien cela va-t-il me coûter ?	Ces audits externes payants ne sont pas si nombreux. Ils vous permettent aussi de réduire ou d'éviter d'autres audits de clients. Le coût peut être limité si vous allez directement à l'essentiel.
C	15	Est-il nécessaire d'être certifié pour une entreprise PME/ETI ?	Non, une entreprise peut capitaliser sur la norme pour décrire, mettre en place et sous contrôle son SMCA sans le faire certifier. La certification apporte néanmoins une reconnaissance ou une assurance officielle de la mise en œuvre d'un SMCA, sous contrôle permanent.

C	16	Comment s'assurer que la norme ISO 22301 est mise en œuvre ?	Dans tous les cas, même sans objectif final de certification, la vérification de la mise sous contrôle d'un SMCA, type 22301, peut passer par un audit, effectué par un organisme extérieur neutre, qui relèvera les points de non-conformité ainsi que le plan d'actions correctives correspondant. En fonction du résultat, la direction générale confirmera ensuite son objectif de certification ISO 22301 ou non et affectera ou non des moyens additionnels pour combler les manques.
C	17	Si je mets en place un PCA et SMCA, mon assureur va-t-il me baisser la prime que je paie ?	Ce dispositif doit surtout vous permettre d'améliorer votre couverture d'assurance ou de mieux maitriser les tarifs. Votre assureur doit le comprendre, sinon, c'est également le moyen de revoir vos contrats d'assurance. Donc, à priori, une mise en œuvre de la norme et une certification devraient influer dans le bon sens.
C	18	J'entends parler de certifications de personnes et d'entreprises. De quoi s`agit-il?	Une entreprise peut faire certifier son SMCA par un organisme tiers certificateur accrédité. Mais elle peut aussi rechercher à ne certifier que quelques personnes clés. Il s'agit alors de faire certifier la compétence ISO 22301 des personnes via une formation agréée suivie d'un examen par un certificateur accrédité.

Annexe 2 – Lexique

Cette annexe recense les termes majeurs les plus utilisés, liés à la continuité d'activité. Les explications ci-dessous proviennent du « Lexique structuré de la continuité d'activité » qui est consultable sur le site du CCA www.clubpca.eu.

1. BIA – Business Impact Analysis - Bilan d'impact sur l'activité :

   - Processus d'analyse des activités et de l'effet qu'une perturbation de l'activité peut avoir sur elles.

2. CCD / CCO – Cellule de Crise Décisionnelle / Cellule de Crise Opérationnelle :

   - Selon la taille de l'entreprise concernée, on peut distinguer Cellule de Crise Décisionnelle (CCD) et Cellule de Crise Opérationnelle (CCO) pour l'activation des PCAs et la mise en œuvre des initiatives décidées par la CCD.

3. Crise :

   La crise est la conséquence d'un événement plutôt que l'événement lui-même. On parle de situation de crise.

4. DMIA – (Délai Maximum d'Interruption Admissible) :

   - «Délai au-delà duquel l'entreprise s'expose à des pertes sérieuses. Délai après lequel les systèmes, applications ou les activités doivent être rétablis après une interruption (ex : 2 heures ; un jour ouvrable).

5. PCA – (Plan de Continuité d'Activité) - Attention ne pas confondre dans ce document avec PDCA :

   - Un PCA définit et identifie l'ensemble des moyens (organisation, procédures et matériels) requis pour se tenir prêt à faire face à un sinistre ou à une avarie majeure. Ces moyens doivent permettre d'assurer la continuité de service et le retour en mode normal dans les meilleurs délais possibles.

6. PDCA – (Plan – Do – Check – Act) :

   - Démarche du modèle qualité PDCA (PLAN-DO-CHECK-ACT) ou roue de Deming utilisé dans la mise en œuvre et le suivi du SMCA.

7. Plan de secours :

   - Un plan de secours définit l'ensemble des procédures et dispositions prévues pour garantir à l'entreprise la reprise de son système informatique en cas de sinistre. Il s'agit d'un sous-ensemble du PCA qui couvre les moyens informatiques et télécom. Il garantit la reprise des systèmes désignés comme critiques dans le temps minimum fixé.

8. PMDT – Perte Maximale de Donnée Tolérable dans le BIA :

   - Source : AFNOR (Perte de Données Maximale Admissible - PDMA)

   Pour une application quelle est la perte acceptable au niveau des données (liée aux sauvegardes) pour que celle-ci soit d'un niveau acceptable pour les services utilisateurs. Selon les besoins exprimés, le degré de fraîcheur des données correspond à la perte des données considérées comme acceptable entre l'arrêt de l'activité et sa reprise. Par exemple, au démarrage après sinistre, les données peuvent dater de la veille au soir, du matin ou de la minute du sinistre.

9. Procédure / Mode opératoire :

   - Une procédure est une manière spécifiée d'effectuer une activité ou un processus.

   Il s'agit aussi du document décrivant l'enchainement des tâches à effectuer dans une situation particulière, par exemple : évacuation, repli, prise en main d'un équipement de repli, etc.

   La procédure est à distinguer du mode opératoire qui décrit dans le détail, la manière de faire fonctionner l'outil mentionné dans une tâche de la procédure.

10. Sinistre :

    Le terme générique de sinistre utilisé dans ce document est la conséquence d'un d'événement perturbateur – événement majeur – catastrophe - etc.

11. SMCA – (Système de Management de la Continuité d'Activité) :

    - Le SMCA est une partie du système de management global d'une entreprise qui en particulier établit, met en œuvre, opère, contrôle, révise, maintient et améliore la continuité d'activité.

> Adhérez au CCA et rejoignez-nous …

L'adhésion au CCA est ouverte à tous. Elle est validée par le bureau du CCA, sous réserve d'acceptation des principes de déontologie énoncés dans le règlement intérieur.

Pour plus d'informations, consulter notre site : www.clubpca.eu

CCA

73 rue Anatole France
92300 Levallois-Perret - France
contact@clubpca.eu