

Table des matières

Avant-propos	1
À qui s'adresse cet ouvrage ?	2
Structure de l'ouvrage	2
Remerciements	3

Partie I – L'entreprise dans un monde de risques

Chapitre 1 – La maîtrise du risque	7
Appréciation des risques	8
Identification des menaces	8
Conséquences sur les actifs de la société	15
Chiffrage des probabilités annuelles	18
Calcul du risque	19
Analyse contrastée par entités	22
Autres méthodes d'analyse pratiquées	24
Évaluation des options face aux risques	26
Les quatre options de traitement du risque	26
Le chiffrage coût/efficacité	29
L'aversion au risque	31
Le dossier d'étude des risques	33
Prise de décision	34
Réévaluation des options par le comité décisionnaire	34
Documentation de l'ensemble	35
Mise en œuvre des options	35
Suivi et contrôle des plans d'actions	36
Les scénarios de sinistre	36
Chapitre 2 – L'analyse d'impact sur les activités	39
Chronologie d'un sinistre	39
Déroulement d'un sinistre	39
Du point de vue de l'utilisateur... ..	42

Cadrage de l'analyse	43
Déterminer les activités critiques	44
<i>Un exercice difficile</i>	44
<i>Identifier les activités</i>	45
<i>Estimer les impacts financiers et opérationnels</i>	46
<i>Identifier les processus critiques</i>	47
Déterminer les configurations	49
<i>MTD et priorités</i>	49
<i>Le facteur temps</i>	51
<i>Systèmes et applications informatiques critiques</i>	52
<i>Ressources humaines et autres ressources critiques</i>	54
Déterminer les paramètres de reprise	54
RTO et WRT	55
Ajustements sur les MTD	56
RPO	57
<i>Procédures de secours</i>	59
Documentation de l'analyse d'impact sur les activités	60
Chapitre 3 – Le développement d'une stratégie de continuité	63
Phase 1 – Expression des besoins en termes de reprise	64
<i>Exigences des processus critiques</i>	64
<i>Étude des besoins</i>	64
Phase 2 – Étude des options possibles pour la reprise	68
<i>Catégories d'options ouvertes</i>	68
<i>Options envisagées</i>	69
Phase 3 – Confrontation des options aux exigences métier	73
<i>Importance de la confrontation</i>	74
<i>Définition des délais d'activation</i>	75
<i>Comparaison aux exigences et sélection des options</i>	80
Phase 4 – Étude de coût et faisabilité	81
<i>Critères d'évaluation</i>	82
<i>Chiffrage des options</i>	82
<i>Sélection d'options</i>	83
Phase 5 – Mise au point de la stratégie de continuité	84
<i>La réactualisation nécessaire de la stratégie</i>	84

Partie II – L'entreprise élabore son plan de continuité

Chapitre 4 – PCA : définir les missions et les responsables	89
Cadrage du plan de continuité	89
<i>Définition du sinistre</i>	89
<i>Objectifs du plan</i>	90
<i>Périmètre et exclusions</i>	91
<i>Contexte général du plan</i>	92
<i>Documentation du plan de continuité</i>	93
<i>Planning des activités</i>	95
Le centre de gestion de crise	96
<i>Un rôle clé</i>	96
<i>Emplacement stratégique du centre de gestion de crise</i>	98
<i>Centre de gestion de crise de secours</i>	98
<i>Fonctions du centre de gestion de crise</i>	99
<i>Équipement du centre de gestion de crise</i>	101
Missions, équipes et responsabilités	101
<i>Le groupe de gestion de crise</i>	102
<i>Le groupe de redémarrage des activités</i>	105
<i>Le groupe de récupération technique et opérationnelle</i>	106
<i>Les listes de contacts</i>	109
Constituer les groupes d'intervention	111
<i>Affectation des missions</i>	112
<i>Former et sensibiliser les différents acteurs</i>	113
<i>Mettre à jour la constitution des groupes</i>	114
Documents types	115
<i>Plan de communication</i>	115
<i>Plan de secours</i>	116
Chapitre 5 – PCA : planifier les activités	117
Planning général en sept étapes	117
<i>Étape 1 – Première intervention et notification du sinistre</i>	118
<i>Étape 2 – Évaluation et escalade</i>	120
<i>Étape 3 – Déclaration de sinistre</i>	121
<i>Étape 4 – Planifier la logistique d'intervention</i>	123
<i>Étape 5 – Récupération et reprise</i>	125
<i>Étape 6 – Retour à la normale</i>	138

Étape 7 – Bilan d'après sinistre	142
Comment affecter les tâches ?	143
Spécificité du PCA	143
Charges et délais cibles	144
Du réalisme avant tout	144
Chapitre 6 – Tester le plan de continuité	147
Cadrage des tests	147
Objectifs	147
Méthodes de test	150
Faut-il annoncer le test ?	153
Document de préparation	154
Contraintes des tests	155
Élaborer un plan de test	155
Phase 1 – Revue des tests antérieurs	155
Phase 2 – Description des objectifs, périmètre et contraintes	156
Phase 3 – Définition de la tactique de test	158
Phase 4 – Mise en place de la logistique de test	162
Phase 5 – Planning et calendrier	164
Phase 6 – Revue des risques du test	165
Phase 7 – Documentation du plan	165
Exécuter les tests	166
Rôle et action des testeurs	166
Consignation des constatations	167
Bilan des tests	168
Suivi des actions d'amélioration	169

Partie III – L'ingénierie de la continuité

Chapitre 7 – Construire la disponibilité	173
Notions statistiques	173
Disponibilité	173
Fiabilité et réparabilité	174
Les modèles redondants	177
Le modèle n+1	178
Prise en compte de la panne de mode commun	178

Arrêts de fonctionnement	180
<i>Arrêt planifié</i>	180
<i>Impact de l'arrêt</i>	181
Site secondaire et site distant	182
<i>Le duo primaire-secondaire</i>	182
<i>Le site distant</i>	183
<i>En réalité...</i>	184
Types d'architectures	184
<i>Architecture monolithique</i>	184
<i>Architecture granulaire</i>	185
<i>Une réalité multiple</i>	185
Chapitre 8 – L'informatique au centre de données	187
Les serveurs	187
<i>Serveurs à tolérance de panne</i>	187
<i>Mise en grappe</i>	188
<i>Virtualisation</i>	190
Le stockage	191
<i>Fonctions des contrôleurs</i>	192
<i>Fonctions du middleware</i>	194
<i>Stockage en réseau NAS</i>	197
<i>Sauvegarde et restauration</i>	198
Les réseaux du centre informatique	202
<i>Réseau de stockage SAN</i>	203
<i>Réseau traditionnel</i>	203
<i>Performance et fiabilité des réseaux</i>	204
Chapitre 9 – Infrastructure et poste de travail de l'employé	205
Les réseaux	205
<i>Réseau téléphonique</i>	205
<i>Réseau informatique</i>	208
Le poste de travail	210
<i>Une importance variable</i>	210
<i>Protection des données</i>	211
<i>Protection des applications</i>	212
<i>Comment continuer à travailler ?</i>	212
<i>Cas des PC portables</i>	213
<i>Travail à domicile</i>	213

Les ressources humaines	214
<i>La malveillance</i>	214
<i>L'aide aux victimes</i>	215
Chapitre 10 – Le centre informatique	217
Choix du site	217
<i>Vulnérabilité du site</i>	218
<i>Attractivité du site</i>	218
<i>Climat des affaires</i>	219
<i>Règles de précaution</i>	219
Infrastructure du centre informatique	220
<i>Éléments critiques</i>	220
<i>Référentiels et normalisation</i>	220
Les principaux risques et leur parade	222
<i>Incendie</i>	222
<i>Dégât des eaux</i>	224
<i>Dysfonctionnements électriques</i>	226
<i>Autres risques</i>	227
Les nouveaux centres : le cloud computing	229
<i>Matériel</i>	229
<i>Fonctionnement</i>	229
<i>Utilisation</i>	230
<i>Perspectives</i>	230
Chapitre 11 – Le plan de continuité en cas de pandémie	231
Les scénarios de risque	231
<i>Les décisions des autorités</i>	231
<i>Le scénario résultant</i>	232
Les activités critiques	233
<i>La notion « d'importance vitale »</i>	233
<i>Un contexte des activités modifié par la pandémie</i>	234
<i>Conséquences sur les moyens sous-jacents</i>	234
Quelles mesures pour un PCA spécial pandémie ?	235
<i>Définir les objectifs stratégiques</i>	236
<i>Établir un classement des missions</i>	237
<i>Prendre en compte des scénarios d'absentéisme à 25 % et à 40 %</i>	238
<i>La préparation à la crise pandémique</i>	240
<i>La protection du personnel</i>	244

<i>Activités transverses</i>	245
<i>Validation du plan</i>	246
<i>Les ressources externes</i>	246
Aspects de gouvernance	246
<i>La construction du plan</i>	247
<i>Le déclenchement</i>	250

Partie IV – La gouvernance de la continuité

Chapitre 12 – La politique de continuité	255
Exprimer une volonté	255
1. <i>Résumé</i>	256
2. <i>Introduction</i>	256
3. <i>Conditions d'application</i>	256
4. <i>Objet</i>	256
5. <i>Périmètre</i>	256
6. <i>Décisions</i>	257
7. <i>Bénéfices attendus</i>	257
8. <i>Responsabilités</i>	257
9. <i>Références</i>	258
Nommer un comité de pilotage et un RPCA	258
<i>Le comité de pilotage</i>	258
Chapitre 13 – Construire et maintenir le plan de continuité	261
Lancement du projet de PCA	261
Formation et sensibilisation	262
<i>Formation des chefs de projet</i>	262
<i>Sensibilisation générale</i>	263
Coordination	263
Le projet de mise en œuvre du PCA	264
Maintenance du PCA	265
<i>Un processus difficile</i>	265
<i>Veille des changements</i>	266
<i>Politique de test nécessaire</i>	266
<i>Prise en compte des conclusions d'audits</i>	270
<i>Gestion des changements du plan</i>	271

Chapitre 14 – Le système de contrôle	273
Objectifs	273
<i>Définir une structure de référence</i>	273
<i>Déterminer les objectifs</i>	274
<i>Décliner les objectifs</i>	276
Évaluer le plan	277
Tirer les conclusions	278
Recommencer	278
La certification du PCA	279
<i>La certification de conformité</i>	279
<i>La réalité de terrain</i>	280
Annexe 1 – Normes et référentiels	281
Les normes internationales	281
<i>Normes de type « bonnes pratiques »</i>	281
<i>Travaux de l'ISO</i>	283
La situation en France	285
<i>Travaux de l'AFNOR</i>	285
<i>Le Club de la Continuité d'Activité (CCA)</i>	285
<i>Le Forum tripartite « joint forum »</i>	286
Les approches connexes	286
ITIL	287
<i>Mehari</i>	287
NFPA 1600	287
Annexe 2 – Sources d'information	289
<i>Organismes francophones</i>	289
<i>Organismes anglophones</i>	289
Index	291

Avant-propos

Un grand nombre d'entreprises ne survivraient pas à une interruption de leur système d'information pendant seulement trois jours. À l'heure où les sinistres semblent se multiplier, des approches nouvelles, organisationnelles et techniques, se sont développées pour faire face aux conséquences et assurer la permanence des activités jugées critiques de l'entreprise.

Le management de la continuité d'activité permet ainsi de rendre l'entreprise plus résiliente dans un monde de risques. Autrefois limitée à la « gestion de crise » ou considérée comme une sous-partie de la gestion des risques ou de la sécurité, cette approche commence à s'imposer comme une discipline à part entière.

Or les observateurs s'accordent à considérer que la continuité d'activité n'a pas actuellement en France l'attention qu'elle mérite de la part des directions générales. En effet, focalisée sur des analyses de risques théoriques, l'entreprise néglige souvent l'impact réel des sinistres potentiels et ne connaît pas les processus les plus critiques. En l'absence de ces considérations, toute atteinte à l'intégrité des moyens vitaux de l'entreprise est souvent chèrement payée par incapacité à réagir efficacement face à l'imprévu.

Certes, quelques plans de reprise d'activité existent ici ou là et l'on peut louer les pionniers qui s'y consacrent. Malheureusement, il s'agit le plus souvent de scénarios trop simples, centrés sur quelques moyens autrefois identifiés comme vitaux et conçus sans vision d'ensemble. En outre, des directions de l'entreprise ont tendance à mettre en place des solutions locales qui, en l'absence d'une vision d'ensemble sur les services essentiels, laissent des lacunes importantes. Dans un monde où les moyens techniques se multiplient et se banalisent, les quelques investissements consentis pour la continuité peuvent ainsi apparaître comme inadaptés si l'on considère la faiblesse de certains maillons organisationnels.

Confiance exagérée dans une technologie fragile, défiance désabusée pour les dispositifs d'organisation utiles, le vécu de la continuité d'activité en France reste largement insatisfaisant. Une prise de conscience des apports réels du management de la continuité d'activité s'impose : c'est l'objectif de cet ouvrage, qui aborde les aspects méthodologiques aussi bien que la mise en œuvre concrète en s'appuyant sur des exemples et situations vécues édifiantes.