

PLAN DE CONTINUITÉ D'ACTIVITÉ ET SYSTÈME D'INFORMATION

Vers l'entreprise résiliente



Matthieu Bennasar

Préface de Paul Théron

2^e édition

DUNOD

Table des matières

Préface	V
Avant-propos	XVII
Première partie – Manager la continuité d'activité	
Chapitre 1 – La problématique et les acteurs de la continuité d'activité	3
1.1 Quelques faits et chiffres	3
1.1.1 <i>Le risque majeur face aux sinistres de notre temps</i>	3
1.1.2 <i>Le coût et la criticité des interruptions de SI</i>	4
1.1.3 <i>La situation des entreprises françaises, comparées au reste du monde</i>	4
1.1.4 <i>Un benchmarking français sur la maturité des entreprises en termes de PCA...</i>	5
1.1.5 <i>Quelques exemples frappants</i>	5
1.1.6 <i>Bilan</i>	7
1.2 <i>Se préparer au pire : une vision pessimiste du monde ?</i>	7
1.3 <i>Contours et domaines de la continuité d'activité</i>	10
1.3.1 <i>Une approche holistique du management</i>	11
1.3.2 <i>Gouvernement d'entreprise, management des risques et continuité d'activité ...</i>	12
1.3.3 <i>Le plan de continuité d'activité : une définition</i>	13
1.3.4 <i>De l'incident au sinistre majeur</i>	14
1.3.5 <i>Ce qui n'est pas du ressort de la continuité d'activité</i>	15

1.4	La réglementation et quelques normes.....	15
1.4.1	La réglementation.....	15
1.4.2	Les normes et standards.....	19
1.4.3	Autres réglementations et normes.....	24
1.4.4	Synthèse.....	26
1.5	PCA, PRA, PCO, PCM, PSI, PGC, etc. : qu'en est-il ?.....	27
1.5.1	Une terminologie en quête de normalisation.....	27
1.5.2	Proposition de définitions.....	27
1.5.3	Tableau comparatif.....	29
1.6	Les acteurs.....	29
1.6.1	La direction générale.....	29
1.6.2	Le risk manager.....	29
1.6.3	Les directions métier.....	31
1.6.4	Le Responsable du PCA (RPCA).....	31
1.6.5	Le Responsable de la sécurité du système d'information (RSSI).....	32
1.6.6	Responsabilités et niveau hiérarchique.....	32
Chapitre 2 – Décider la mise en place de la continuité d'activité.....		35
2.1	Un projet d'entreprise.....	35
2.1.1	Mandat et sponsor.....	35
2.1.2	Pilotage de la démarche.....	36
2.1.3	Conduite du changement.....	36
2.1.4	Régime établi.....	37
2.1.5	Se faire aider ou pas ?.....	37
2.1.6	Quelques écueils courants.....	38
2.2	Décider de mettre en place un PCA.....	44
2.2.1	Les bonnes raisons de mettre en place un MCA.....	44
2.2.2	Quelques préalables.....	47
2.2.3	Les quatre principaux composants d'un PCA.....	47
2.2.4	Le ROI par construction.....	48
2.2.5	Le « ROI » inquantifiable.....	51
2.2.6	Quelques conseils aux décideurs.....	54

Deuxième partie – Méthodes et outils de la continuité d'activité

Chapitre 3 – Mettre en place la continuité d'activité : méthodologie commentée .	63
3.1 Démarche générale.....	63
3.1.1 De l'« expertise » en continuité d'activité.....	63
3.1.2 Les principaux composants d'un dispositif de continuité d'activité	64
3.1.3 La démarche E = MCA en six phases	65
3.1.4 Notes sur le formalisme utilisé pour décrire la méthodologie	66
3.2 Phase 1 – Mieux connaître son activité : l'étape décisive	67
3.2.1 Étape 1.A : cartographie et scénarios de sinistres	67
3.2.2 Étape 1.B : Bilan d'Impact sur l'Activité (BIA)	69
3.2.3 Étape 1.C : Analyse des Risques (AR)	72
3.2.4 Première étape facultative de la phase 1 : analyse de couverture des contrats d'assurances.....	74
3.2.5 Deuxième étape facultative de la phase 1 : diagnostic de prévention.....	75
3.3 Phase 2 – Orienter la stratégie de continuité d'activité.....	77
3.3.1 Étape 2.A : stratégie globale de continuité	77
3.3.2 Étape 2.B : stratégie locale de continuité	78
3.3.3 Étape 2.C : choix des solutions techniques de continuité	80
3.4 Phase 3 – Développer le Plan de continuité d'activité (PCA).....	82
3.4.1 Étape 3.A : Plan de Gestion de Crise (PGC)	82
3.4.2 Étape 3.B : plans transverses (PU, GP, PR)	86
3.4.3 Étape 3.C-1 : Plan de Continuité Métier (PCM)	87
3.4.4 Étape 3.C-2 : Plan de Continuité du SI (PCSI)	88
3.5 Phase 4 – Mettre en place les solutions fonctionnelles et techniques de continuité.....	90
3.5.1 Étape 4.A : mise en place des infrastructures de continuité	90
3.5.2 Étape 4.B : Procédures Fonctionnelles de Continuité (PFC).....	92
3.5.3 Étape 4.C : Procédures Informatiques de Continuité (PIC)	93
3.5.4 Étape 4.D : test des dispositifs techniques de continuité.....	94
3.6 Phase 5 – Déployer et maintenir en conditions opérationnelles	96
3.6.1 Étape 5.A : sensibilisation, formation et communication	97
3.6.2 Étape 5.B : maintien en conditions opérationnelles du PCA	99
3.6.3 Étape 5.C : test du PCA.....	100

3.6.4	Étape 5.D : contrôle du PCA.....	102
3.7	Phase 6 – Piloter le management de la continuité d'activité.....	104
3.7.1	Étape 6.A : pilotage du projet PCA.....	104
3.7.2	Étape 6.B : pilotage du MCA.....	105
3.8	Synoptiques récapitulatifs de la méthodologie E = MCA.....	107
3.9	Quelques cas particuliers.....	116
3.9.1	Le secteur banques et finance.....	116
3.9.2	Le secteur PME/PMI.....	116
3.9.3	Le secteur public.....	117
3.9.4	Le SI infogéré.....	118
Chapitre 4	Panorama des solutions techniques de secours.....	119
4.1	Les solutions de secours des moyens informatiques.....	119
4.1.1	Solutions de secours du SI.....	120
4.1.2	Typologie des moyens de secours (SI) : avantages et limites.....	120
4.1.3	De la bonne distance du site de secours (SI).....	123
4.1.4	Disponibilité des solutions : conséquences sur les principaux composants de la chaîne SI.....	124
4.1.5	Mener l'analyse coûts/bénéfices et avantages/inconvénients sur les solutions de secours (SI).....	124
4.1.6	Le marché et les principaux fournisseurs de services et solutions de secours (SI).....	126
4.1.7	Un mot sur l'aspect contractuel du secours informatique.....	128
4.2	Les solutions de secours des moyens de production.....	130
4.2.1	Une problématique bien différente de celle du SI !.....	130
4.2.2	Axes de réflexion et retours d'expérience.....	131
4.3	Les solutions de secours des locaux et équipements.....	132
4.3.1	Sauvetage des locaux et équipements.....	132
4.3.2	Secours des locaux et équipements.....	132
4.4	Le secours des ressources humaines.....	133
4.5	Les systèmes d'information du MCA(SIMCA).....	134
4.5.1	Où l'on définit un SIMCA.....	134
4.5.2	Les fonctionnalités d'un SIMCA.....	135
4.5.3	Quelques raisons pour mettre en place un SIMCA.....	135
4.5.4	Critères de succès pour la mise en œuvre d'un SIMCA.....	136

102	4.5.5 Quelques outils.....	136
104	4.5.6 Le coût d'un SIMCA intégré.....	137
104	4.6 La question des coûts du secours.....	138
105	4.6.1 Aspects financiers liés à la mise en place de la partie fonctionnelle d'un plan de continuité d'activité.....	138
107	4.6.2 Ordres de grandeur financiers pour la solution technique de secours (SI).....	141
116		
116	Chapitre 5 – Considérations techniques sur les solutions de secours.....	145
116	5.1 Sauvegarde, restauration et disponibilité des données.....	145
117	5.1.1 Méthodes de sauvegarde.....	147
118	5.1.2 Cas particuliers de sauvegarde.....	148
119	5.1.3 Technologies de sauvegarde et architecture de haute disponibilité des données... ..	149
119	5.1.4 Critères de choix des solutions de sauvegarde.....	156
120	5.2 Considérations techniques sur les composants critiques du SI : stratégies de secours.....	157
120	5.2.1 Serveurs.....	158
123	5.2.2 Réseau local.....	159
124	5.2.3 Réseau WAN.....	160
124	5.2.4 Sites web.....	161
124	5.3 Considérations techniques sur les outils et moyens périphériques.....	162
126	5.3.1 Postes et stations de travail.....	162
128	5.3.2 Téléphonie.....	164
130	5.3.3 Impression.....	164
130	5.3.4 Internet.....	165
131	Chapitre 6 – Études de cas.....	167
132	6.1 Cas n° 1 – Mise en place d'un plan de continuité informatique local.....	167
132	6.1.1 L'énoncé du problème.....	168
132	6.1.2 L'approche proposée et la démarche mise en œuvre.....	169
133	6.1.3 Étape 1 – Mieux connaître l'activité.....	169
134	6.1.4 Étape 2 – Orienter la stratégie de continuité.....	171
134	6.1.5 Étape 3 – Mettre en place la solution technique de continuité.....	171
135	6.1.6 Conclusion.....	172
135	6.2 Cas n° 2 – Audit d'un plan de continuité informatique et définition du PCA ..	172
136	6.2.1 L'énoncé du problème.....	173

6.2.2	<i>L'approche proposée et la démarche mise en œuvre</i>	174
6.2.3	<i>Les livrables et les résultats</i>	176
6.2.4	<i>Conclusion</i>	178
6.3	<i>Cas n° 3 – Mise en place d'un plan de continuité métier (PCM)</i>	179
6.3.1	<i>L'énoncé du problème</i>	180
6.3.2	<i>L'approche proposée et la démarche mise en œuvre</i>	181
6.3.3	<i>Étape 1 – Mieux connaître l'activité</i>	182
6.3.4	<i>Étape 3 : Développer le plan de continuité d'activité</i>	191
6.3.5	<i>Étape 5 – Assurer la conduite du changement, le déploiement du PCM et son maintien en conditions opérationnelles</i>	196
6.3.6	<i>Conclusion</i>	201
6.4	<i>Cas n° 4 – Retour d'expérience pour une crise majeure : les attentats de Londres</i>	201

Troisième partie – Perspectives

Chapitre 7 – Vers un système de management de la continuité d'activité et une entreprise résiliente ?	205
7.1 <i>Les principaux systèmes de management de l'entreprise</i>	206
7.1.1 <i>Qualité (ISO 9001)</i>	206
7.1.2 <i>Sécurité et santé au travail (OHSAS 18001)</i>	206
7.1.3 <i>Environnement (ISO 14001)</i>	206
7.1.4 <i>Sécurité de l'information (ISO 27002 et ISO 27001)</i>	207
7.1.5 <i>Éthique et responsabilité sociale (SA 8000)</i>	207
7.1.6 <i>Systèmes propres à l'entreprise</i>	207
7.2 <i>L'intégration des divers systèmes de management : vers un SMI</i>	208
7.2.1 <i>Les concepts intégrateurs</i>	208
7.2.2 <i>La construction du tronc commun</i>	212
7.2.3 <i>Les avantages</i>	212
7.3 <i>Proposition d'un Système de management de la continuité d'activité (SMCA)</i>	214
7.3.1 <i>Un système de management de la continuité d'activité</i>	214
7.3.2 <i>Vers le management unifié ?</i>	214
7.4 <i>Vers la résilience</i>	216
7.4.1 <i>Vous avez dit résilience ?</i>	216
7.4.2 <i>Construire la résilience</i>	217

174
176
178
179
180
181
182
191
196
201
201

205
206
206
206
206
207
207
207
208
208
212
212
214
214
214
216
216
217

7.5 Conclusion..... 219

Conclusion..... 221

ANNEXES

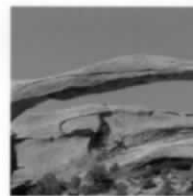
Annexe A – Sigles et abréviations 227

Annexe B – Quelques illustrations documentaires de la méthodologie 229

Annexe C – Les démarches connexes et les méthodes associées 275

Références bibliographiques 291

Index 299



Matthieu Bennasar

Préface de Paul Théron

PLAN DE CONTINUITÉ D'ACTIVITÉ ET SYSTÈME D'INFORMATION

Vers l'entreprise résiliente

Cet ouvrage s'adresse aux décideurs de l'entreprise ainsi qu'aux maîtres d'œuvre de la continuité d'activité (RPCA, risk managers, RSSI et DSI).

Le **management de la continuité d'activité** permet de préparer l'entreprise à faire face aux crises qui peuvent paralyser ses activités. Il se matérialise notamment par un **plan de continuité d'activité** (PCA) pragmatique, à jour et testé.

Structuré en trois parties, cet ouvrage actualisé sur les normes européennes donne une vision stratégique de la continuité d'activité :

- La première partie est destinée aux décideurs qui y trouveront les **grands principes du management de la continuité d'activité**.
- La deuxième partie propose une **méthodologie** en vue d'assurer la continuité d'activité avec le détail des étapes de sa **mise en œuvre** : bilan d'impact sur l'activité (BIA), analyse des risques, tests du PCA... Elle présente aussi des **études de cas**.
- La troisième partie trace les **perspectives d'évolution**, du management de la continuité d'activité vers la résilience d'entreprise.

« Cette nouvelle édition tient largement compte des évolutions de la discipline, notamment en France. Elle apportera une aide certaine à tous ceux qui doivent développer en détail des plans de continuité. Les études de cas sont extrêmement bien ciblées et développées avec précision. J'apprécie tout particulièrement le nouveau chapitre sur la résilience qui est évidemment le devenir de la gestion de la continuité d'activité. »

Pierre-Dominique LANSARD

Vice-président du Club de la Continuité d'Activité

MANAGEMENT DES SYSTÈMES D'INFORMATION

APPLICATIONS MÉTIERS

ÉTUDES, DÉVELOPPEMENT, INTÉGRATION

EXPLOITATION ET ADMINISTRATION

RÉSEAUX & TÉLÉCOMS

2^e édition

MATTHIEU BENNASAR

MBCI et CISM

Ancien auditeur informatique chez PricewaterhouseCoopers, il est aujourd'hui manager responsable de l'offre Résilience & Continuité d'Activité du groupe LEXSI.

Il est chargé de cours à l'IAE de Lyon et à l'IMI, et membre du BCI.



La première édition de cet ouvrage a reçu le prix AFISI 2006 du meilleur livre informatique de langue française.

