

NORME BRITANNIQUE

BS 25999-2

Management de la continuité d'activité – Partie 2

Spécification



NORME BRITANNIQUE

Management de la continuité d'activité – Partie 2: Spécification



CETTE PUBLICATION NE PEUT ÊTRE REPRODUITE À L'EXCEPTION DE CE QU'AUTORISE LE DROIT D'AUTEUR

Information relative à l'édition et au droit d'auteur

La notice de droit d'auteur de BSI figurant dans ce document indique la date de la dernière édition de ce document.

© BSI 2010

ISBN 978 0 580 62941 9

ICS 03.100.01

Les références BSI suivantes se rapportent au travail réalisé sur la présente norme:

Référence de la commission BCM/1

Avant-projet pour observations 07/30145272 DC

Précédentes éditions

Première édition Novembre 2007

Amendements apportés à la première édition

Amend. N°	Date	Texte concerné
-----------	------	----------------

Sommaire

Avant-propos *ii*

Introduction 1

1 Domaine d'application 4

2 Termes et définitions 4

3 Planification du SMCA 9

3.1 Généralités 9

3.2 Etablissement et gestion du SMCA 9

3.3 Intégration du MCA dans la culture de l'organisme 11

3.4 Documentation et enregistrements relatifs au SMCA 11

4 Mise en œuvre et fonctionnement du SMCA 12

4.1 Comprendre l'organisme 12

4.2 Détermination de la stratégie de la continuité d'activité 14

4.3 Développement et mise en œuvre des réponses dans le cadre du MCA 14

4.4 Exercice, maintenance et revue des dispositions du MCA 16

5 Surveillance et revue du management du SMCA 17

5.1 Audit interne 17

5.2 Revue de direction du SMCA 18

6 Maintenance et amélioration du SMCA 19

6.1 Actions préventives et correctives 19

6.2 Amélioration continue 20

Annexes

Annex A (informative) Correspondance entre BS EN ISO 9001:2000, BS EN ISO 14001:2004, BS ISO/IEC 27001:2005 21

Bibliographie 23

Liste des figures

Figure 1 – Cycle PDCA appliqué aux processus du SMCA 2

Figure 2 – Le cycle de vie du management de la continuité d'activité (MCA) 3

Liste des tableaux

Tableau A.1 – Correspondance entre BS 25999-2 et d'autres normes de système de management 21

Synthèse des pages

Ce document comprend une page de couverture, une deuxième de couverture, les pages i à ii, les pages 1 à 24, une troisième de couverture et une quatrième de couverture.



Documents

Document Sharing Hub

© BSI 2010 • 1

Avant-propos

La présente Norme britannique a été publiée par BSI et est entrée en vigueur le 20 Novembre 2007. Elle a été conçue par le Groupe d'experts BCM/1/-/2, sous l'autorité de la Commission Technique BCM/1, *Management de la continuité d'activité*. Une liste des organismes représentés au sein de cette commission peut être demandée à son secrétariat.

La présente Norme britannique a été élaborée par des juristes appartenant à l'ensemble de la communauté du secteur de la continuité d'activité en mettant à profit leurs expériences universitaires, techniques et pratiques en matière de management de la continuité d'activité. Elle a été créée pour déterminer les exigences d'une approche du système de management appliquée au management de la continuité d'activité basé sur les bonnes pratiques utilisées par les organismes de grande, moyenne et petite tailles travaillant dans les secteurs industriels, commercial, public et du bénévolat.

BS 25999, *Management de la continuité d'activité* comporte deux parties:

- *Partie 1: Code de bonne pratique;*
- *Partie 2: Spécification.*

Les exigences spécifiées dans la présente Norme britannique ont été élaborées en prenant en compte les principes et pratiques contenus dans BS 25999-1.

La présente Norme britannique offre une spécification qui peut être utilisée par des parties internes et externes, y compris les organismes de certification, afin d'évaluer la capacité de l'organisme à satisfaire les exigences de la réglementation, des clients et de l'organisme lui-même.

La présente Norme britannique ne contient que les exigences qui peuvent être objectivement vérifiées. Les organismes nécessitant des conseils plus généraux sur toute une gamme de questions touchant au management de la continuité d'activité se référeront à la BS 25999-1.

Une démonstration d'une mise en œuvre réussie de la présente Norme britannique peut ainsi être utilisée par un organisme pour assurer aux parties concernées qu'un système approprié de management de la continuité d'activité est en place.

Tout comme les normes modernes de système de management, la présente norme utilise le cycle « Planifier-Faire-Vérifier-Agir » («PDCA») pour développer, mettre en œuvre et améliorer l'efficacité du système de management de la continuité d'activité d'un organisme.

La présente publication n'a pas la prétention de comprendre toutes les dispositions essentielles d'un contrat. Les utilisateurs sont responsables de son emploi convenable.

Le respect de la Norme britannique n'implique pas l'exonération des obligations légales.

Introduction

Généralités

La présente Norme britannique spécifie les exigences pour la mise en œuvre et la gestion d'un système de management de la continuité d'activité efficace (SMCA).

Ceci souligne l'importance:

- a) de comprendre les besoins de continuité de l'activité et la nécessité d'établir une politique et des objectifs pour une continuité d'activité;
- b) de mettre en œuvre et d'appliquer des dispositifs de contrôle et des mesures afin de gérer l'ensemble des risques de la continuité d'activité d'un organisme;
- c) de surveiller et d'examiner la performance et l'efficacité du SMCA; et
- d) de l'amélioration continue basée sur des mesures objectives.

Un SMCA, comme tout autre système de management, possède les composants clés suivants:

- a) une politique;
- b) des personnes aux responsabilités définies;
- c) des processus de management relatifs à:
 - 1) la politique;
 - 2) la planification;
 - 3) la mise en œuvre et le fonctionnement;
 - 4) l'évaluation de la performance;
 - 5) la revue de direction; et
 - 6) l'amélioration;
- d) un ensemble de documents fournissant des preuves contrôlables; et
- e) des processus de projet spécifiques relatifs à la question, en l'occurrence, la continuité d'activité, tels que l'analyse d'impact sur les affaires (AIA) et le développement du plan de la continuité d'activité.

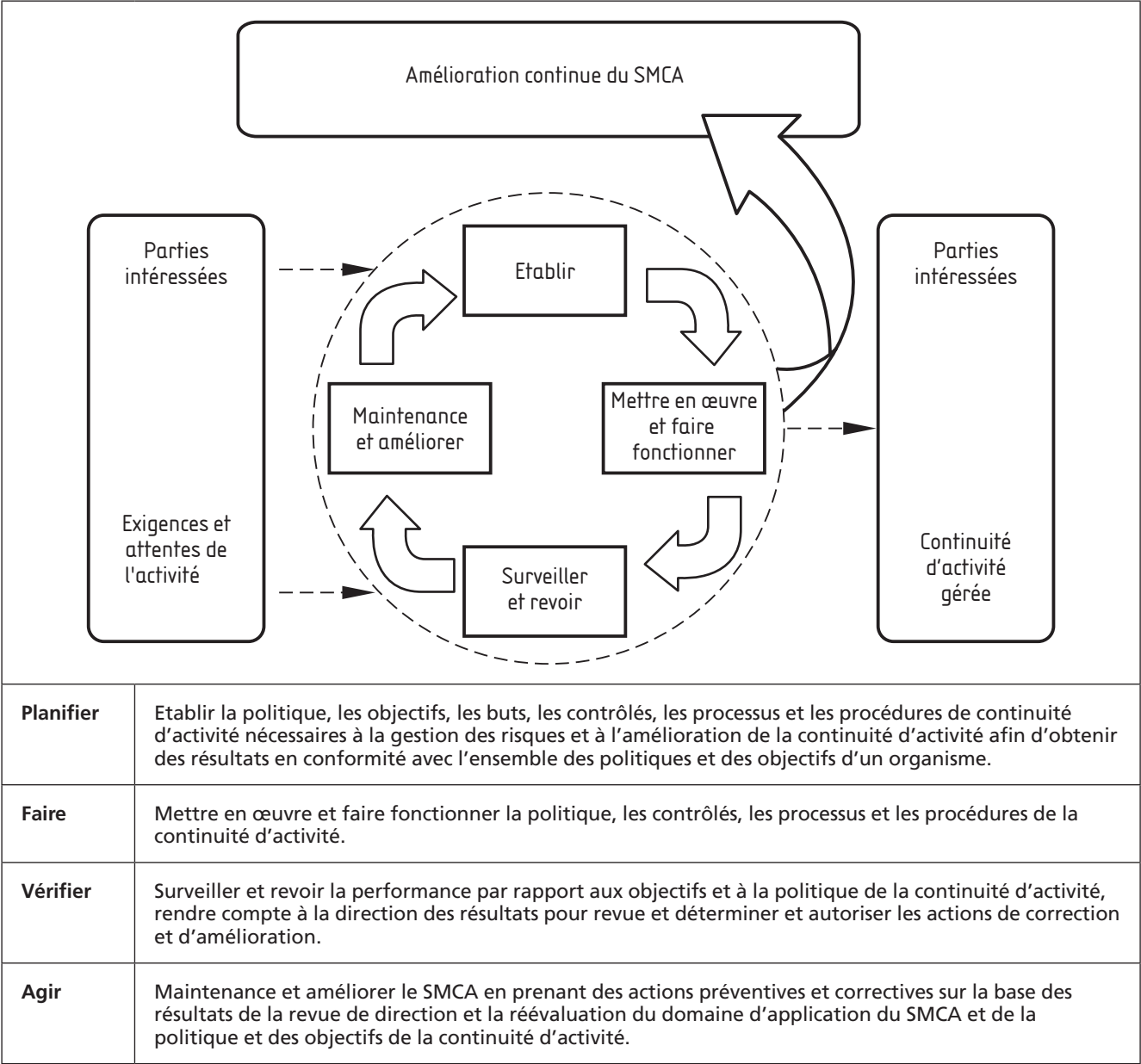
Le cycle « Planifier-Faire-Vérifier-Agir » («PDCA»)

La norme applique le cycle « Planifier-Faire-Vérifier-Agir » («PDCA») pour établir, mettre en œuvre, faire fonctionner, surveiller, pratiquer les exercices, maintenance et améliorer l'efficacité du SMCA.

Ceci assure une certaine cohérence avec les autres normes de système de management, telles que BS EN ISO 9001:2000 (systèmes de management de la qualité), BS EN ISO 14001:2004 (systèmes de management environnemental), BS ISO/IEC 27001:2005 (systèmes de management de la sécurité de l'information) et BS ISO/IEC 20000:2005 [management des services des technologies de l'information (TI)], renforçant en conséquence la mise en œuvre et le fonctionnement harmonieux et intégrés avec les systèmes de management correspondants (voir Annexe A).

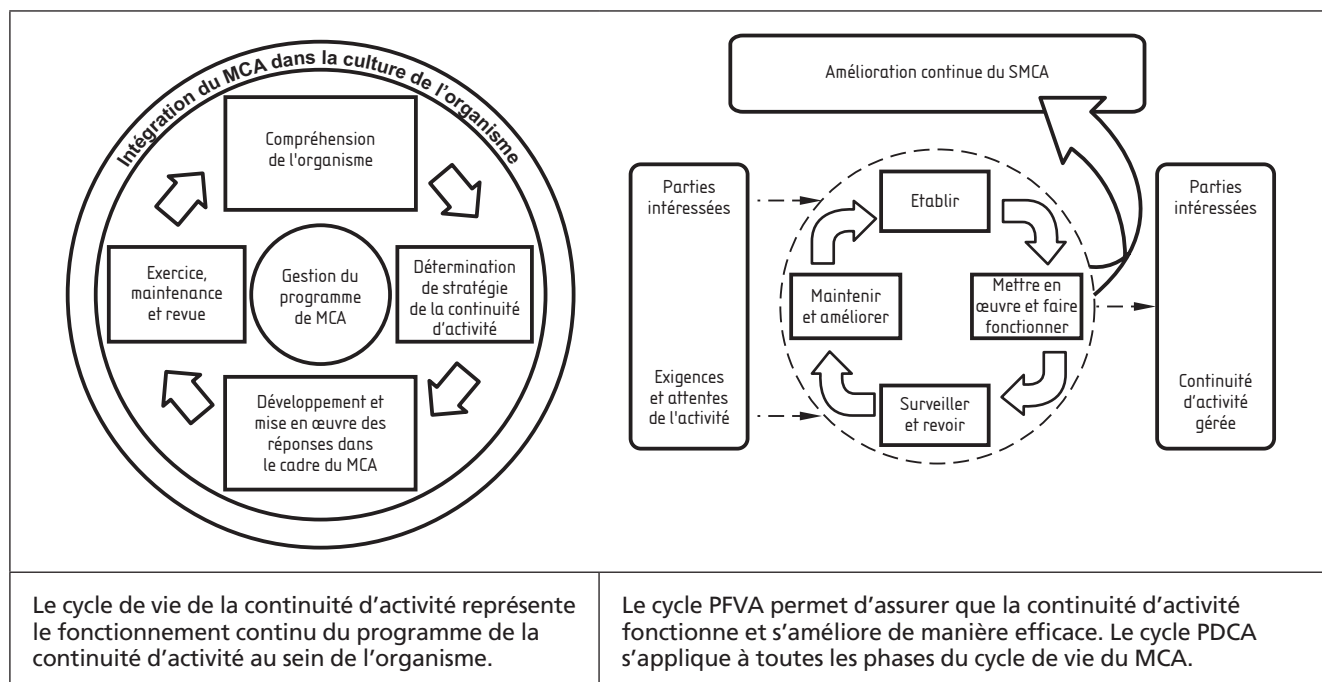
La Figure 1 illustre comment le SMCA considère comme des éléments d’entrée les exigences et les attentes de continuité d’activité des parties concernées et, par l’utilisation d’actions et de processus nécessaires, produit des résultats de continuité d’activité (c’est-à-dire, la continuité d’activité gérée) qui répondent à ces exigences et attentes.

Figure 1 Cycle PDCA appliqué aux processus du SMCA



Une approche largement admise et qui englobe le cycle PDCA au sein de chaque activité est recommandée dans BS 25999-1 et décrite succinctement à la Figure 2. Ce processus itératif assure que la continuité d’activité est établie et gérée en continu au sein d’un organisme (pour une explication de chaque élément du cycle de management de la continuité d’activité, voir BS 25999-1:2006, 3.7).

Figure 2 Le cycle de vie du management de la continuité d'activité (MCA)



1 Domaine d'application

La présente Norme britannique spécifie les exigences pour la planification, l'établissement, la mise en œuvre, le fonctionnement, la surveillance, la revue, l'exercice, la maintenance et l'amélioration d'un système de management de la continuité d'activité (SMCA) documenté dans le cadre du gestion de l'ensemble des risques d'activité d'un organisme.

Les exigences spécifiées dans la présente Norme britannique sont génériques et prévues pour s'appliquer à tout organisme (ou à certaines parties de celui-ci), quels que soient le type, la taille et la nature de l'activité. L'étendue de l'application de ces exigences dépend de l'environnement d'exploitation et de la complexité de l'organisme.

La présente Norme britannique n'a pas pour but d'impliquer l'uniformité dans la structure d'un SMCA mais plutôt d'élaborer un SMCA qui réponde aux besoins de l'organisme et qui soit conforme aux exigences des parties prenantes. Ces besoins sont déterminés par les exigences de la réglementation, des clients et de l'activité, par les produits et services, par les processus utilisés, par la taille et la structure de l'organisme et par les exigences des parties prenantes.

La présente Norme britannique peut être utilisée par les parties internes et externes, y compris les organismes de certification, pour évaluer la capacité de l'organisme à satisfaire ses exigences de continuité d'activité, ainsi que les exigences des clients, de la réglementation ou de la loi.

2 Termes et définitions

Pour les besoins de cette partie de la BS 25999, les définitions suivantes s'appliquent.

2.1 activité

processus ou ensemble de processus engagé par un **organisme** (ou pour son compte) qui produit ou soutient un ou plusieurs produits ou services

NOTE Des exemples de ces processus sont le service comptable, le centre d'appels, le service des TI, la fabrication, la distribution.

2.2 audit

vérification systématique pour déterminer si les activités et les résultats correspondants sont conformes aux mesures prises et si ces mesures sont mises en œuvre de manière efficace et sont adaptées à la réalisation de la politique et des objectifs de l'organisme

[BS EN ISO 9000:2005]

2.3 continuité d'activité

capacité stratégique et tactique de l'organisme à prévoir les **incidents** et les **interruptions** d'activité et à y répondre afin de poursuivre l'exploitation d'activité à un niveau prédéfini admissible

2.4 management de la continuité d'activité (MCA)

processus global de management qui identifie les menaces potentielles envers un organisme et les **impacts** sur l'exploitation d'activité que ces menaces, si elles se réalisaient, pourraient avoir, et qui offre une structure afin de fournir une **faculté de récupération** par l'organisme