Fiche Pratique

CRiP Digital Technology & Innovation

Club des Responsables d'Infrastructures et de Production

En partenariat avec CCA Club de la Continuité d'Activité

PRA - PCA

L'audit de la continuité d'activité d'un organisme

Pour être sûre et valide, la continuité d'activité nécessite une évaluation

La continuité d'activité correspond à la capacité d'un organisme (entreprise ou administration) à poursuivre son fonctionnement et l'atteinte de ses objectifs à un niveau acceptable défini par avance, suite à la survenance d'un évènement perturbateur.

L'audit s'appuie sur un référentiel et sur les normes existantes : ISO 22301, ISO 27001, etc. La profondeur et la précision de l'audit sont étroitement liées au niveau de maturité de l'organisme audité en matière de continuité d'activité.

La continuité d'activité doit être évaluée par les PCA, le Système de Management de la Continuité d'Activité (SMCA) et le service rendu aux clients.

L'audit de la continuité d'activité doit être perçu comme une opération positive et constructive pour l'organisme. Il entre directement dans le processus d'amélioration continue de la Roue de Deming (PDCA) en proposant un plan visant à améliorer la continuité d'activité de l'organisme.

Pour les entreprises de services, la norme ISAE 3402 (évolution de SAS 70) permet de démontrer à ses clients la conformité de son organisation à leurs exigences réglementaires en matière financière. Elle permet d'éviter les audits de PCA par les clients de ces entreprises.

Les trois domaines cibles d'évaluation de la continuité :

Les trois domaines cibles d'évaluation de la continuité :

- Le Plan de Continuité d'Activité (PCA),
- Le Système de Management de la Continuité d'Activité (SMCA) (cf. norme certifiante ISO 22301 publiée en mai 2012),
- Les services rendus à ses clients (cf. International Standard on Assurance Engagements (ISAE 3402, évolution de SAS 70), norme internationale publiée en décembre 2009 par l'International Auditing and Assurance Standards Board (IAASB), qui fait partie de la Fédération Internationale des Comptables (IFAC).

Cela nécessite l'utilisation d'un vocabulaire commun entre l'audité et l'auditeur. Le Lexique structuré de la continuité d'activité du Club de la Continuité d'Activité (CCA) propose des définitions admises par la profession.

NB. : L'audit de la gestion de crise n'a pas été traité dans cette fiche pratique.

Mai 2014

Introduction

L'audit aide l'organisme à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle et de gouvernance, et en faisant des propositions pour renforcer leur efficacité (source : définition adoptée le 21/03/2000 par le Conseil d'Administration de l'IFACI, Institut Français de l'Audit et du Contrôle Internes).

Trois formes d'audit existent :

. l'audit interne,

. l'audit externe,

. l'audit de certification.

Les critères d'audit du Plan de Continuité d'Activité (PCA)

Comment peut-on évaluer le caractère opérationnel d'un PCA ?

Les critères d'évaluation suivants sont à prendre en compte :

	Oui	Non
1. Expression de besoin des processus métier et support (aux métiers)		
a. Les processus métier et support ont-ils exprimé leurs besoins de continuité d'activité ?		
b. Les besoins et les dispositifs de continuité ont-ils été validés par la Direction de l'organisme ?		
c. Les plans de retour à une situation normale ont-ils été prévus ?		
d. Les besoins exprimés dans le BIA (Bilan d'Impacts sur l'Activité) font-ils partie du contrat de service ?		
e. Le niveau de dégradation d'activité suite au sinistre a-t-il été défini et validé ?		

2. Degré de couverture du PCA en termes d'impacts sur le fonctionnement de l'organisme		
a. Est-ce que les risques ont été analysés et leurs impacts évalués ?		
b. Toutes les dépendances externes (tierces parties) à l'organisme ont-elles un PCA conforme aux besoins validés par la Direction Générale ?		
c. A-t-on pris en compte toutes les exigences légales et réglementaires inhérentes au secteur d'activité ?		
d. Les risques sur les activités ont-ils été validés par la Direction Générale ?		
e. Les priorités de reprise d'activité sont-elles clairement définies ?		
f. Les impacts des risques communs entre l'organisme et ses fournisseurs externes critiques ont-ils été pris en compte ?		

3. Moyens de continuité		
a. Les responsabilités d'exécution du PCA ont-elles été définies pour tous les acteurs aux différentes étapes (construction et exécution) ?		
b. Les salles de crise, en particulier leurs moyens de communication, sont-elles secourues ?		
c. Les moyens de communication entre tous les acteurs sont-ils suffisants ?		
d. Les moyens de secours et de repli sont-ils non impactés par les scénarios prévus d'indisponibilité des ressources ?		
e. Les moyens de continuité ont-ils été identifiés et justifiés pour être mis en œuvre en conformité avec les besoins exprimés et validés ?		

4. Efficacité du PCA : adéquation des besoins de continuité aux réponses techniques		
a. Les conditions de reprise d'activité observées (RTO, RPO, positions de repli et de stock) sont-elles conformes aux conditions attendues par les processus métier et support en termes de délai de reprise, perte de données, positions de repli et de stock ?		

	Oui	Non
b. Les moyens de secours et de repli sont-ils suffisamment dimensionnés pour assurer les besoins de continuité validés ?		
c. La cellule de crise décisionnelle est-elle unique ?		

5. Documentation et outils du PCA		
a. Y a-t-il un système de gestion documentaire ?		
b. La documentation du PCA est-elle accessible immédiatement quoi qu'il arrive ?		
c. La documentation est-elle exhaustive et à jour : contacts, fiches réflexe, procédures (toute la documentation nécessaire pour exécuter le PCA) ?		
d. Le PCA est-il exécutable par d'autres personnes compétentes qui n'ont pas écrit les procédures ?		
e. Y a-t-il un plan de coordination de l'exécution du PCA ?		
f. Les informations du PCA sont-elles classifiées et leur diffusion est-elle contrôlée (habilitations définies) ?		

6. Maintien en condition opérationnelle		
a. Les changements du SI, des locaux, de l'organisation fonctionnelle, sont-ils répercutés dans le PCA ?		
b. Disposez-vous de processus de contrôle autres que les tests techniques et exercices de validation ?		
c. Y a-t-il un processus de formation continue du personnel de l'organisme ?		
d. Y a-t-il à l'issue des tests et exercices un retour d'expérience et un plan d'amélioration du PCA ?		
e. Le plan de validation prévoit-il une progressivité des tests et exercices sur plusieurs années ?		
f. Y a-t-il des exercices de validation inopinés ou avec un minimum de préparation ?		

7. Pilotage d'exécution du PCA		
a. Tous les décideurs de la cellule de crise décisionnelle sont-ils entraînés au pilotage de crise ?		
b. Y a-t-il des critères d'aide à la décision pour déclencher ou non le PCA ?		
c. Les communications interne et externe sont-elles préparées par type de scénarios de risques ?		

8. Degré d'implication du personnel impliqué dans le PCA		
a. Toutes les parties prenantes (interne et externe) du PCA sont-elles formées, entraînées, et savent-elles ce qu'elles doivent faire en cas de besoin ?		
b. Tous les intervenants sont-ils en nombre suffisant en permanence (7j/7, 24h/24) ?		
c. La formation des personnes a-t-elle été prévue ?		

Les critères d'audit du Système de Management de la Continuité d'Activité (SMCA)

La gestion de la continuité d'activité est un processus de management holistique qui identifie les menaces potentielles pour un organisme ainsi que les impacts que ces menaces, si elles se concrétisent, peuvent avoir sur les opérations liées à l'activité de l'organisme. Ce même processus fournit un cadre pour construire la résilience de l'organisme avec une capacité de réponse efficace préservant les intérêts de ses principales parties prenantes, sa réputation, sa marque et ses activités productrices de valeur (norme ISO 22301 Système de Management de la Continuité d'Activité).

Les critères d'évaluation du SMCA sont classés selon les thèmes de la Roue de Deming :

	Oui	Non
1. Plan (planifier)		
a. Y a-t-il un périmètre défini pour le SMCA ?		
b. Y a-t-il un engagement de la Direction (sponsoring) ?		
c. Le SMCA fait-il l'objet d'une politique de l'organisme ?		
d. Les exigences légales et réglementaires sont-elles prises en compte ?		
e. Les ressources projet (Responsable PCA, Correspondant PCA, contributeurs) sont-elles définies ?		

2. Do (mettre en œuvre)		
a. Avez-vous mis en œuvre un plan de communication interne et externe ?		
b. Le BIA et la stratégie de continuité sont-ils réalisés ?		
c. L'analyse et le traitement des risques en termes d'impacts ont-ils été réalisés ?		
d. Le Groupe de pilotage de la continuité est-il constitué ?		
e. Le PCA est-il construit ?		

3. Check (vérifier)		
a. A-t-il été mis en œuvre un processus de contrôle du PCA ?		
b. Les exercices sont-ils réalisés conformément à la politique de continuité ?		
c. Les compétences des personnes en charge du PCA sont-elles évaluées périodiquement ?		
d. Y a-t-il un plan de suivi des indicateurs de performance du PCA ?		
e. Un processus d'audit interne existe-t-il ?		

4. Act (agir/ajuster)		
a. La révision du SMCA prend-t-elle en compte les écarts constatés entre le « Do » et le « Check » ?		
b. Un plan d'amélioration continue existe-t-il ?		

Les critères d'audit des services rendus aux clients, selon la norme ISAE 3402, au regard du PCA

La norme ISAE 3402 (International Standard on Assurance Engagements) offre aux entreprises de services qui sont soumises à la loi Sarbanes-Oxley (ou à d'autres lois de sécurité financière), la possibilité de certifier la conformité de leur organisation aux exigences réglementaires. Cette norme est portée par l'IAASB (International Auditing and Assurance Standards Board), organisme qui fait lui-même partie de l'IFAC (International Federation of Accountants).

Le recours à la norme ISAE 3402 s'inscrit dans un processus comprenant plusieurs étapes. L'entreprise doit d'abord formaliser précisément son dispositif de contrôle interne, ses objectifs de contrôle et les contrôles associés, puis établir un document décrivant l'ensemble de ce dispositif. C'est sur la base de ce document que l'auditeur rédigera son rapport.

En pratique, il existe deux types de rapports :

- Un rapport de type I, dans lequel l'auditeur vérifie la bonne description des contrôles et leur adéquation par rapport aux objectifs fixés. Ce rapport est effectué une fois par an, à un moment donné ;
- Un rapport de type II, dont l'objectif est de vérifier l'efficacité opérationnelle des contrôles décrits dans le rapport de type I, sur une période de six mois (en général).

Ce dernier rapport comprend quatre sections :

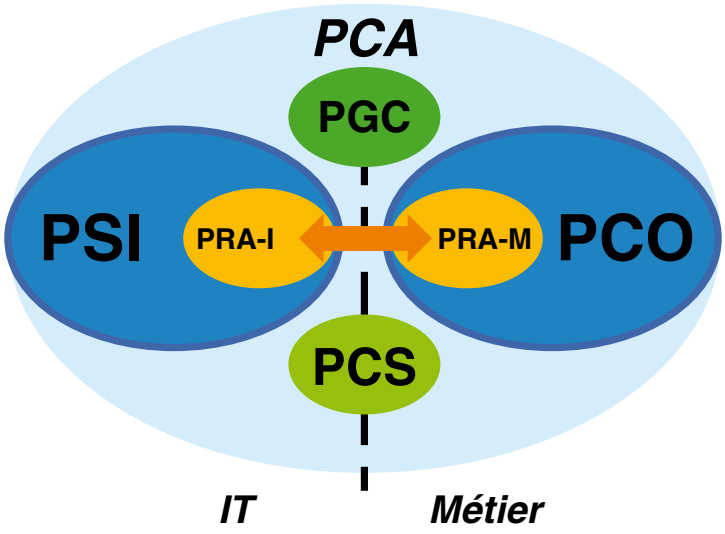
1. Le rapport de l'auditeur proprement dit,
2. La description des contrôles,
3. La description des tests effectués par l'auditeur ainsi que leurs résultats,
4. Autres informations fournies par l'entreprise prestataire de services (facultatif).

La certification **ISAE 3402 de type II** est donc la certification la plus complète. Elle intègre non seulement un audit au moment de la certification, mais ensuite des contrôles réguliers pour s'assurer que les procédures mises en place restent bien appliquées. Pour chaque service audité, une grille de contrôle a été mise en place avec une liste des objectifs de contrôle, des activités contrôlées, des plans de tests, des observations et recommandations.

Extrait des recommandations de l'AICPA (American Institute of Certified Public Accountants) :

Si une entreprise prestataire de services souhaite décrire son PCA, elle doit le faire dans la section 4 (Autres informations fournies par l'entreprise prestataire de services), car un plan n'est pas un contrôle.

Les différents sous-ensembles du PCA



Un plan de continuité d'activité (PCA) est constitué de 6 sous-ensembles : PGC, PCS et PSI, PCO.

Sigle	Intitulé	Périmètre	Objectif
PCA	Plan de Continuité d'Activité	Organisme	Assurer la résilience de l'organisme
PCO	Plan de Continuité des Opérations	Activités métier critiques	Assurer le fonctionnement acceptable des activités critiques
PCS	Plan de Continuité des Services	Partie(s) de l'organisme concernée(s) par la crise	Protection et disponibilité des ressources
PGC	Plan de Gestion de Crise	Partie(s) de l'organisme concernée(s) par la crise	Assurer une gestion maîtrisée du pilotage des plans
PSI	Plan de Secours Informatique	Le Système d'Information	Assurer le secours des fonctions centrales du SI
PRA-I	Plan de Reprise d'Activité - Informatique	Le Système d'Information	Reprise de l'activité du SI après interruption
PRA-M	Plan de Reprise d'Activité - Métier	Activités métier critiques	Rendre l'activité métier

3. Conclusion

L'audit de la continuité d'activité couvre, outre les ripostes prévues par les scénarios de risques (PCA), le management et l'organisation de la continuité d'activité. Il offre une vision globale de la préparation et du fonctionnement de l'organisme en cas de sinistre, car il interroge sur :

- la criticité des processus métier,
- la couverture des procédures de continuité d'activité,
- la mise à jour de ces procédures face aux nouveaux contextes et référentiels.

L'audit interne, qui sert à rassurer la Direction sur la bonne maîtrise de ses risques et la résilience de l'organisme, doit être associé à un audit externe qui lui est complémentaire. A ce titre, il a le regard tourné vers les interactions extérieures, car il atteste de la sécurisation des activités auprès les parties prenantes et permet, en cas de conformité du Système de Management, d'obtenir une certification ISO 22301 (sécurité sociétale et management de la continuité d'activité).

La nouvelle norme ISO 22301 présente bien des avantages pour l'organisme certifié :

- Elle s'intègre aisément aux autres systèmes de management présents dans l'organisme,
- Elle l'inscrit dans un processus d'amélioration continue en questionnant sur l'adaptabilité du système face aux nouveaux enjeux,
- Elle crée un rapport de confiance entre les parties prenantes et ledit organisme,
- Elle permet d'étayer les réponses aux appels d'offre lorsque la problématique de la continuité d'activité est abordée.

Il est néanmoins important de signaler que les auditeurs n'émettent qu'une recommandation de certification, laquelle n'est prononcée que par un organisme certificateur habilité.

Annexe et liens utiles

- Définition des termes employés : Lexique structuré de la continuité d'activité, version 3, du Club de la Continuité d'Activité (www.clubpca.eu)
- Guide pour réaliser un Plan de Continuité d'Activité, SGDSN, 2013 (www.sgdsn.gouv.fr/site_article128.html)
- ISAE 3402 (www.isae3402.com)

Rédaction : Groupe de Travail PRA-PCA - Pilotes François Tête - CCA, Pascal Antier - ADP GSI - Création Fred.lameche - www.anousdejouer.fr

Club des Responsables d'Infrastructures et de Production
24 rue Erlanger 75016 Paris - contact@crip-asso.fr www.crip-asso.fr

Club de la Continuité d'Activité
73 rue Anatole France 92300 Levallois Perret - contact@clubpca.eu www.clubpca.eu