Spécificité des Systèmes d'Information
Validation d'un PCA

François TÊTE
Président d'honneur du CCA
Consultant Devoteam

Pourquoi et comment élaborer un Plan de Continuité d'Activité ?
19/01/2017

Constats

1. Un Plan de Continuité d'Activité PCA insuffisamment validé à toutes les chances de ne pas fonctionner; créant des difficultés de prise de décision et un impact sur l'organisme.

2. Le caractère probant de la validation ne peut être atteint à 100 %.

3. On peut s'en approcher régulièrement par des tests et exercices réguliers et probants.

   – Que veut dire probant ?
   – Quels sont les critères de qualification d'un exercice PCA ?
   – Quels sont les critères pour réussir la validation ? .

Les objectifs de la validation d'un PCA

- S'entraîner en vue d'un éventuel événement perturbateur,
- S'assurer de l'efficacité des dispositifs de continuité d'activité,
- Prouver la capacité de continuité d'activité vis-à-vis de tiers,
- Promouvoir l'image du PCA auprès de la Direction Générale,
- Former et sensibiliser les acteurs concernés,
- Contrôler le Maintien en Condition Opérationnelle du PCA,
- Corriger les points faibles identifiés lors d'une précédente validation.

Des modalités de validation

- Des tests techniques
- Des exercices d'entrainement
- Un exercice peut être :
  - simulé ou réel,
  - préparé ou impromptu.

Trois règles :
1- Prendre des précautions

- Avoir vérifié les prérequis et effectué les tests techniques avant l'exercice
- Vérifier que les sauvegardes spécifiques à l'exercice ont été effectuées pour des retours arrière certains
- Avoir l'aval de la Direction sur les risques encourus
- Avoir l'aval des Métiers pour les périodes « permises » de l'exercice
- Limiter les erreurs humaines toujours possibles (validations collégiales, utilisation de scripts, …)

5

Trois règles :
2 - Opter pour des validations progressives

- Commencer par identifier ce que l'on va tester
- Faire un ensemble de validation sur des périmètres cohérents bien définis
- Progresser ensuite sur des ensembles et volumes plus importants
- Tester l'organisation cible prévue en cas de crise
- Multiplier les exercices dans des conditions diverses avec des personnes différentes
- Progresser vers des exercices inopinés en limitant les préparations

6

Trois règles :
3 - Impliquer la Direction Générale

- La Direction Générale doit imposer des scénarios de risques à traiter, sur propositions de la DSI et du Responsable du PCA
- La Direction Générale doit valider les conditions de réalisation d'exercices :
  - Simulés ou réels
  - Préparés ou inopinés
  - A quelles dates ? Sur quelles durées ?
  - Sur quels périmètres ?

Critères pour qualifier un test / exercice probant (1/2)

1 - Le périmètre des validations successives du PCA est-il adéquat aux niveaux de services issus du BIA fait avec les métiers ?

2 - Le scénario de risque pris en compte dans l'exercice était-il réaliste ? (Ce cas peut-il arriver ?)

3 - Les conditions d'arrêt simulant le sinistre comportaient-elles assez d'éléments aléatoires pour être proches d'un cas réel ?

4 - Le scénario de risque a-t-il été validé par la direction des risques ou son équivalent ?

5 - L'exercice a-t-il eu une préparation limitée ?

6 - Les conditions de reprise d'activité observées sont-elles conformes aux conditions attendues par les métiers ?

7 - L'entrainement des décideurs et des opérationnels (internes et externes) est-il suffisant ?

Critères pour qualifier un test / exercice probant (2/2)

8 - Est-ce que les dernières mises à jour de l'environnement ont été prises en compte et testées dans le PCA ?

9 - Les exercices ont-ils été « rejoués » par des personnes différentes ?

10 - Les conditions de « stress » des participants étaient-elles adéquates ?

11 - Les exercices ont-ils révélé des erreurs ? Ces erreurs doivent être diagnostiquées.

12 - La durée de l'exercice a-t-elle été suffisante pour caractériser un scénario de sinistre réaliste ?

13 - L'exercice a-t-il produit des preuves auditables ? Ont-elles été conservées ?

14 - Le test/exercice a-t-il été contrôlé par des observateurs internes ou externes indépendants ?

Les bonnes pratiques pour obtenir un exercice probant

- Une implication de la Direction Générale
- Une forte implication de toutes les parties prenantes
- Un niveau de services convenu à celui attendu
- Un périmètre d'applications bien défini et significatif
- Une série de tests / exercices itératifs et auditables
- Une capitalisation des exercices pour industrialisation
- Une préparation limitée
- Des conditions de reprise proches d'un cas réel
- Très peu de personnes au courant du contenu de l'exercice
- Un exercice inopiné

Conclusion

- Il faut que la compagne de validation s'intègre dans un processus d'amélioration continue (Roue de Deming).

- Plus le PCA fait l'objet d'exercices qui tendent vers un caractère probant, plus la confiance s'installe, participant à l'accroissement de son niveau de maturité.

- L'industrialisation ou l'automatisation partielle ou globale du PCA permet de garantir son exécution, et de gagner en efficience.