
COMMUNIQUÉ

16-COM-002

1^{er} août 2016

Publication d'un guide de planification de la reprise après sinistre

L'Association des superviseurs prudents des caisses (ASPC) a publié un guide de planification de la reprise après sinistre (PRS) qui décrit les processus, les politiques et les procédures éclairés liés à la reprise ou à la continuité des infrastructures essentielles à une organisation après une catastrophe d'origine naturelle ou humaine.

Ce guide est destiné à sensibiliser les coopératives de crédit et les caisses populaires aux notions de PRS et à aider les responsables des TI à élaborer et à mettre en œuvre des plans de reprise après sinistre au sein de leurs organisations.

Chaque territoire de l'ASPC peut choisir d'appliquer les orientations dans leur forme actuelle ou modifiée, à sa discrétion.

L'ASPC restera à l'affût des recherches et des orientations nationales et internationales en matière de PRS afin d'améliorer en permanence les pratiques de gestion des risques des caisses de crédit et des caisses populaires du Canada.

À propos de l'ASPC

L'Association des superviseurs prudents des caisses (ASPC) est un regroupement interprovincial composé d'organismes d'assurance-dépôts et de superviseurs prudents répartis dans l'ensemble du Canada. L'ASPC œuvre à maintenir le caractère sain et durable du secteur des caisses canadiennes, au moyen d'actions concertées. Pour plus de renseignements, consultez le site Web de l'ASPC, www.cupsa-aspc.ca.

Guide de planification de la reprise après sinistre

La planification de la reprise après sinistre (PRS) désigne les processus, politiques et procédures liés à la reprise ou à la continuité des infrastructures essentielles à une organisation après une catastrophe d'origine naturelle ou humaine.

Pour les besoins du présent document, l'ASPC fournit seulement des conseils en matière de PRS relatifs à la technologie de l'information dans son application à l'ensemble des fonctions de planification de la continuité des activités (PCA).

Cette orientation a été élaborée pour les coopératives de crédit et les caisses populaires pour mieux sensibiliser le milieu aux notions de PRS et aider les responsables qui élaborent et mettent en œuvre des plans de reprise après sinistre au sein de leurs organisations.

Les domaines mentionnés dans le présent document peuvent être adaptés selon la taille, l'envergure, la complexité et le profil de risque des institutions. En plus de ce document, l'ASPC encourage les coopératives de crédit et les caisses populaires à consulter les documents d'orientation rédigés par d'autres organismes de réglementation provinciaux.

La planification de la reprise après sinistre (PRS) et la planification de la continuité des activités (PCA)

La PRS est un sous-ensemble de la PCA et doit englober la planification de la reprise des applications, des données, du matériel, des communications (comme les réseaux) et d'autres infrastructures de TI.

En revanche, la PCA est un programme à l'échelle de l'organisation utilisé pour récupérer et restaurer la fonctionnalité des affaires après une catastrophe ou une interruption prolongée. Cela comprend la planification des aspects non liés aux TI, comme le personnel, les installations, la communication de crise et la protection de la réputation.

Au cours de la PCA, les organisations déterminent le caractère critique de la priorité des fonctions de l'entreprise et établissent des objectifs d'interruption acceptables pour ces fonctions. La planification de la reprise après sinistre a pour but d'établir des processus et des procédures de reprise afin d'atteindre et de dépasser les objectifs et les cibles nécessaires pour maintenir les fonctions commerciales établies durant la planification de la continuité des activités.

Principes et pratiques de la PRS

La planification de la reprise après sinistre doit découler du plan de continuité des activités d'une organisation et se concentrer plus en détail sur l'infrastructure informatique. Elle doit permettre la reprise rapide et sécurisée des applications, des données, du matériel, des communications

(comme les réseaux) et d'autres infrastructures de TI touchés par un scénario de catastrophe ou d'incident. La planification de la reprise après sinistre peut comprendre les éléments suivants :

Évaluation de l'impact technologique

L'organisation doit procéder à une évaluation de l'impact technologique, qui est une évaluation et une analyse des infrastructures existantes nécessaires pour soutenir leurs fonctions essentielles. Cela peut comprendre les éléments suivants :

- Création d'un inventaire de l'infrastructure informatique existante, y compris les ressources informatiques, les bases de données, le stockage, la sécurité, les composants du réseau, le personnel et les fournisseurs (listes des coordonnées des personnes clés);
- Exécution d'une analyse de la défaillance d'un ou plusieurs composants de l'infrastructure informatique de la coopérative de crédit ou de la caisse populaire et de son impact sur une fonction critique;
- Établissement d'objectifs de point de restauration et de temps de reprise pour les applications et les systèmes.

Plan de reprise après sinistre (Plan RS)

Chaque organisation doit établir un plan officiel de reprise après sinistre, qui peut porter sur les éléments suivants :

- coordonnées du personnel clé;
- équipe de reprise après sinistre – définition, rôles et responsabilités;
- documentation à l'appui – documents d'évaluation de l'impact technologique, contrats, accords de niveau de service, coordonnées du personnel clé des fournisseurs, etc.;
- procédures de restauration, y compris :
 - les procédures d'activation et de notification pour signaler quand une catastrophe a été déclarée et comment conserver la circulation des informations;
 - les procédures de réaction aux incidents relatives aux premières étapes de la catastrophe et les mesures à prendre;
 - les procédures d'évaluation des dommages qui déterminent les dégâts subis lors de la catastrophe, et qui se concentrent sur les efforts de restauration;
 - les procédures de réinstallation et de restauration doivent viser à récupérer les applications et les systèmes informatiques critiques. Selon la nature et l'ampleur de la catastrophe, on décidera de reconstruire, de restaurer à partir des sauvegardes ou d'utiliser d'autres méthodes de récupération.

Test du plan RS

Le plan RS d'une organisation doit être testé périodiquement. On acquiert ainsi la confiance et l'expérience nécessaires pour répondre à une urgence réelle. C'est également un moyen d'accroître sans cesse le niveau d'éducation et de sensibilisation en ce qui concerne les situations

et les procédures de sinistres. Les résultats des tests doivent être résumés dans un rapport soumis au conseil d'administration.

Les tests vous aident à garder le plan RS à jour, y compris les coordonnées des personnes clés et les procédures de reprise. Ils peuvent également faire en sorte que les estimations/délais de reprise soient réalistes; aider le personnel à conserver sa familiarité avec le plan; et assurer que les procédures, les sites et les infrastructures de remplacement prévus dans le plan fonctionnent comme prévu.

Sensibilisation et formation

L'organisation doit chercher à créer des plans RS clairs, concis et bien compris par la direction et le personnel. La direction doit promouvoir la sensibilisation aux pratiques de reprise après sinistre et de réponse aux incidents au sein de son organisation. L'équipe de RS doit avoir un niveau raisonnable de formation par rapport à ses responsabilités, et maintenir cette expertise sur une base régulière.

Rôles et responsabilités en matière de PRS

L'ASPC a défini les rôles et les responsabilités clés en matière de PRS comme suit :

Conseil d'administration

- Étudier et approuver les politiques de reprise après sinistre qui favorisent la mise en place, l'entretien et l'essai de la PRS dans l'organisation.
- Étudier les rapports de tests de PRS.

La haute direction

- Affecter les ressources et le personnel adéquats aux processus et aux efforts de reprise après sinistre.
- Faire en sorte qu'un PRS adéquat soit en place, maintenu périodiquement et testé de manière efficace.
- Harmoniser les initiatives et les priorités en matière de PRS et de PCA afin de s'assurer qu'elles se soutiennent efficacement les unes les autres.
- Soumettre des rapports sur la gestion, la maintenance et les tests de PRS de l'organisation au conseil d'administration.

Vérificateurs internes/externes

- Évaluer la conception et l'efficacité de la PRS.
- Confirmer la pertinence de la PRS en termes de protection des actifs et contribuer à la résilience globale de l'organisation.

Fournisseurs de services tiers

- Fournir une confirmation aux coopératives de crédit ou aux caisses populaires quant à la mise en place de produits, de services et d'arrangements internes ou externes de PRS prêts à l'emploi.

Régulateurs

- Fournir une orientation ou des pratiques commerciales éclairées en matière de PRS aux coopératives de crédit et aux caisses populaires.
- Évaluer les PRS des coopératives de crédit et des caisses populaires pour veiller à ce qu'elles suivent les pratiques exemplaires de l'industrie.
- S'assurer que les coopératives de crédit et les caisses populaires établissent et mettent en œuvre des plans d'action si les évaluations révèlent qu'elles ont échoué à se conformer efficacement aux pratiques commerciales efficaces relatives à la planification de la reprise après sinistre.