

Gestion de la continuité des opérations et gestion des incidents de l'entreprise

Déclaration externe



Publication : Mars 2020

Programme de gestion de la continuité des opérations et de gestion des incidents

Le service Gestion de la continuité des opérations et gestion des crises de l'entreprise (GCOGCE) est une fonction essentielle du Groupe Banque TD (la « Banque ») et fait partie intégrante de ses activités d'exploitation habituelles. Cette fonction suit des politiques internes qui sont conformes à la réglementation du secteur. Elle comprend la mise en œuvre, à l'échelle de l'entreprise, de processus de gestion des incidents et de la continuité des opérations qui offrent des mesures de protection visant à réduire au minimum les risques de perturbation des processus et des services d'affaires ainsi que les coûts y afférents et la durée de telles perturbations.

En vue de se préparer en cas d'incidents qui pourraient interrompre nos activités et nos opérations, le programme à l'échelle de l'entreprise permet à la haute direction d'être en mesure de poursuivre la gestion et l'exploitation de ses unités et de fournir aux clients un accès aux produits et aux services. Notre programme très complet comprend des protocoles officiels de gestion des incidents et des stratégies de continuité. La Banque revoit et met à l'essai régulièrement ses plans de continuité des opérations et ses plans de reprise après sinistre afin d'être préparée en cas de perte ou de perturbation de tout élément dont dépendent des fonctions essentielles.

Le programme de gestion de la continuité des opérations et de gestion des incidents de la Banque combine la planification de la reprise des activités, la gestion des incidents et la planification de la remise en état des systèmes. Il est régi par des politiques approuvées par le Conseil qui sont sous la gestion des groupes Solutions technologiques et Gestion du risque opérationnel de la Banque et est conforme aux pratiques professionnelles du secteur de la continuité des opérations.

Planification de la continuité des opérations

Toutes les unités fonctionnelles et fonctions de surveillance sont responsables de la mise en œuvre des pratiques en matière de gestion de la continuité des opérations et de gestion des crises de l'entreprise (GCOGCE), et de l'élaboration de procédures, de plans d'essai et de protocoles propres à une unité fonctionnelle. Toutes les unités fonctionnelles et fonctions de surveillance doivent évaluer leur tolérance au risque et leur vulnérabilité à une interruption des activités en suivant le processus d'analyse des répercussions sur les opérations pour établir le niveau de criticité de l'entreprise, qui permet de déterminer les objectifs de reprise et la rigueur des activités associées à la continuité des opérations. La stratégie de reprise prend en considération la nature, la portée et la complexité de l'unité pour déterminer si elle peut continuer à mener ses activités de façon raisonnable tout en respectant ses diverses obligations en cas d'interruption. Les plans de continuité des opérations renforcent la capacité de reprendre les activités en cas d'interruption défavorable causée par une perte de technologies importantes (y compris des cyberévénements), d'installations, de fournisseur de services tiers, et de la capacité à travailler des employés (y compris les pandémies) en prévoyant les arrangements nécessaires, que ce soit à l'externe ou à l'interne. Nos plans de continuité des opérations sont examinés par les groupes Gestion des affaires et GCOGCE de la Banque conformément aux normes et au niveau de criticité du plan définis par la Banque afin d'assurer leur exactitude, leur qualité et leur conformité.

Exercice de mise à l'essai des plans de continuité des opérations

Toutes les unités doivent mettre à l'essai leurs plans de continuité des opérations conformément à la Politique de gestion de la continuité des opérations et de gestion des crises et des incidents. Les groupes Gestion des affaires et GCOGCE examinent les résultats des exercices et des tests conformément aux normes et au niveau de criticité du plan définis par la Banque. Des exercices doivent être effectués pour déterminer si les mesures prévues sont suffisantes pour atteindre les objectifs de continuité et de reprise. Les critères de réussite des mises à l'essai sont fondés sur les objectifs préétablis afin de respecter les normes minimales de mises à l'essai en matière de continuité des opérations.

Gestion des crises et des incidents (protocoles et exercices)

La Banque maintient un protocole de gestion des crises opérationnelles de l'entreprise, coordonné par le groupe GCOGCE, dans le but de faciliter la supervision, la prise en charge et la gestion efficaces des crises et des incidents qui touchent la Banque. Les protocoles de transmission à une instance supérieure et de communication sont établis, mis à l'essai, revus et coordonnés de concert avec le groupe Gestion des affaires d'assurer le bon fonctionnement du processus décisionnel, des communications internes et externes et de la gestion des médias. Tous les principaux secteurs d'exploitation, comme les définit le groupe GCOGCE, doivent assurer la tenue à jour et la mise à l'essai de leurs protocoles de gestion des incidents conformément aux normes établies de gestion de la continuité des opérations et de gestion des crises de l'entreprise. Il incombe au groupe GCOGCE d'assurer la tenue et la mise à l'essai du protocole de la Banque en matière de gestion des crises de l'entreprise.

Programme de reprise après sinistre

Le Programme de reprise après sinistre de la Banque est géré par le groupe Gestion du risque technologique et Sécurité de l'information de la Banque et comprend une gamme complète de stratégies techniques et de procédures visant à réduire au minimum les répercussions d'une interruption technique et à faciliter le retour à la normale des activités et de la prestation de services.

Le programme vise à encadrer la reprise après sinistre afin de réduire au minimum le risque lié à la remise en état des systèmes, des applications et des données de la Banque, y compris l'infrastructure et les réseaux, et de donner la confiance nécessaire pour assurer cette remise en état. Les applications sont hébergées dans des centres des données internes renforcés, et des solutions de reprise spécialisées sont en place dans un site de reprise appartenant à la Banque.

La fréquence des examens et des essais du plan de reprise après sinistre est proportionnelle au risque lié à la reprise après sinistre. Ces examens et essais sont consignés dans des rapports internes confidentiels.

Conformité à la réglementation

Le programme de GCOGCE de la Banque est conçu pour répondre aux exigences de différents organismes gouvernementaux, de réglementation et de surveillance, ainsi que des normes du secteur, notamment :

Le Bureau du surintendant des institutions financières (BSIF), l'Autorité des marchés financiers (AMF), le Federal Financial Institutions Examination Council (FFIEC), la Réserve fédérale américaine (Fed), la Federal Deposit Insurance Corporation (FDIC), l'Office of the Comptroller of the Currency (OCC), la Financial Industry Regulatory Authority (FINRA), la Financial Conduct Authority, la Prudential Regulation Authority, les Pays-Bas, la Hong Kong Monetary Authority (HKMA) et la Monetary Authority of Singapore (MAS). Le Programme de GCOGCE de la Banque s'appuie également sur des normes internationales, dont la norme ISO 22301.

Conclusion

Les plans de continuité des opérations, les protocoles de gestion des incidents et les plans de reprise après sinistre de la Banque sont documentés, soumis à des exercices et testés, et les résultats¹ sont vérifiés de façon indépendante sur une base régulière. Les programmes de continuité des opérations et de reprise des activités après sinistre appliquent le modèle des trois lignes de défense à la gestion du risque.

La Banque n'obtient pas de rapport d'audit en vertu de la norme SSAE 18. Cependant, en vertu de l'article 404 de la loi Sarbanes-Oxley, nos auditeurs indépendants ont vérifié l'efficacité des contrôles internes de la Banque à l'égard de l'information financière, et ces résultats sont rendus publics puisqu'ils font partie des états financiers consolidés de la Banque.

Nous voulons déployer des efforts commercialement prudents et raisonnables pour assurer la continuité des opérations de la Banque et ses clients. Cependant, nous ne faisons aucune déclaration ni ne donnons aucune garantie selon lesquelles les systèmes de la Banque ne seront touchés par aucun incident. Le présent document se veut un guide sur le programme de GCOGCE et de reprise des activités après sinistre de la Banque; il ne modifie ni ne remplace d'aucune façon toute entente, garantie ou déclaration relative aux produits ou aux services de la Banque, notamment en ce qui a trait à la disponibilité de ces produits ou services. Si elle le juge approprié, la Banque se réserve le droit de modifier sans préavis les procédures et les marches à suivre décrites dans le présent document.

¹ Il est à noter que les évaluations de la Banque et de ses fournisseurs ne sont pas rendues publiques.