Gestion de la continuité des opérations et de gestion des crises et des incidents

Déclaration externe

Publication : Juillet 2022

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

La gestion de la continuité des opérations et la gestion des crises et des incidents sont vitales pour le Groupe Banque TD (« la Banque ») et font partie intégrante de ses activités d'exploitation habituelles. Le programme de gestion de la continuité des opérations et de gestion des crises et des incidents de la Banque est conforme aux politiques internes et conçu pour respecter les règlements du secteur. Il comprend la mise en œuvre, à l'échelle de l'entreprise, de processus de gestion de la continuité des opérations et de gestion des crises et des incidents 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 prévision d'incidents susceptibles de perturber nos activités et nos opérations, le programme de gestion de la continuité des opérations et de gestion des crises et des incidents, établi à l'échelle de l'entreprise, permet à la haute direction 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, de gestion des crises et des incidents et 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 crises et des incidents de la Banque combine la planification de la reprise des activités, la gestion des crises et des incidents et la planification de la reprise des systèmes en fonction de la nature et de la portée des unités et des activités de la Banque, compte tenu de son empreinte opérationnelle, géographique et numérique. Le programme de gestion de la continuité des opérations et de gestion des crises et des incidents est régi par les politiques qui ont reçu l'aval du conseil d'administration, qui sont gérées par les groupes Gestion du risque opérationnel et Bureau du chef de la sécurité de l'information de la Banque, et qui sont conformes aux lignes directrices réglementaires et aux normes du secteur en matière de gestion de la continuité des opérations et de gestion des crises.

Planification de la continuité des opérations

La mise en œuvre des pratiques en matière de gestion de la continuité des opérations et de gestion des crises et des incidents de l'entreprise, de même que l'élaboration de procédures, de plans d'essai et de protocoles propres à une unité fonctionnelle, relèvent de cette unité et des fonctions de surveillance. Toutes les unités fonctionnelles et fonctions de surveillance doivent évaluer leur tolérance au risque et leur vulnérabilité à une perturbation des activités en suivant le processus d'analyse des répercussions sur les opérations afin d'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 pour l'unité ou la fonction en question. La stratégie de reprise d'une unité fonctionnelle ou d'une fonction de surveillance 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 d'une unité fonctionnelle ou d'une fonction de surveillance portent sur la capacité de l'unité ou de la fonction à se remettre d'une perturbation des activités causée par la perte d'une technologie clé (y compris les cyberévénements), d'une installation, d'un ou de plusieurs fournisseurs de services tiers ou de la capacité de travailler d'un employé (y compris en cas de pandémie, d'agitation civile et de catastrophe naturelle). Les plans de continuité des opérations sont appuyés par des dispositions appropriées, qu'ils soient fournis à l'interne ou impartis. Nos plans de continuité des opérations sont examinés par les dirigeants de l'unité fonctionnelle et le groupe Gestion de la continuité des opérations et gestion des crises de l'entreprise de la Banque, conformément aux normes définies en matière de continuité des opérations et de gestion des crises de la Banque (les « normes »), qui en vérifient l'adéquation, le caractère raisonnable, la qualité et la conformité aux normes.

Plans de continuité des opérations – tests et exercices

Toutes les unités fonctionnelles et fonctions de surveillance 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 dirigeants de chaque unité fonctionnelle et le groupe Gestion de la continuité des opérations et gestion des crises de l'entreprise examinent les résultats des exercices et des tests conformément aux normes et au niveau

de criticité du plan définis par la Banque. Des exercices et des tests sont requis pour vérifier que les dispositions respectent les objectifs de continuité et de reprise des activités. Les critères de réussite des exercices et des tests sont fondés sur des objectifs préétablis afin de respecter les normes minimales de mises à l'essai en matière de continuité des opérations. Les grandes leçons apprises et les mesures à prendre déterminées à la suite des exercices et des tests sont intégrées au plan et aux stratégies de reprise pour favoriser l'amélioration continue.

Surveillance de tiers

Toutes les unités fonctionnelles et les fonctions de surveillance doivent avoir mis en place des stratégies et des solutions de rechange appropriées pour répondre aux interruptions prolongées des ententes de services conclues avec des tiers et essentielles à l'entreprise. Les unités fonctionnelles supervisent les plans de continuité des opérations afin qu'ils soient conformes aux normes de la Banque.

Évaluation des risques et des menaces

Chaque année, la Banque examine et évalue les risques potentiels liés à la résilience, notamment en contribuant à l'analyse de scénarios d'atteinte aux opérations et à la cybersécurité, ainsi qu'aux simulations de crise. L'évaluation tient compte de l'exposition de la Banque, y compris les vulnérabilités potentielles aux menaces internes et externes de perturbation des activités. Les unités fonctionnelles et les fonctions de surveillance sont tenues de gérer les principales menaces et les principaux risques relevés dans l'évaluation des menaces et des risques de leurs plans de continuité des opérations.

Gestion des crises et des incidents (protocoles, tests et exercices)

La Banque applique les protocoles de gestion des crises et des incidents au niveau de l'entreprise et de chaque unité fonctionnelle, afin de déterminer l'approche et le processus à utiliser pour répondre efficacement aux événements et aux menaces qui perturbent ses activités. Par exemple, elle réunit les équipes de gestion des crises et des incidents, leurs rôles, leurs responsabilités, leur pouvoir décisionnel, le processus de transmission à un niveau supérieur, les procédures de communication et la mise en œuvre des protocoles de reprise des activités.

Chaque année, les unités fonctionnelles et les fonctions de gestion du risque, de gouvernance et de surveillance doivent effectuer des exercices et des tests de l'état de préparation de leurs protocoles de gestion des crises et des incidents pour valider les processus et les procédures qui servent à gérer les crises et les incidents qui perturbent leurs activités et à y répondre. Les équipes Gestion du risque opérationnel et Gestion de la continuité des opérations et gestion des crises et des incidents de l'entreprise font un examen indépendant et une analyse critique de tous les exercices, tests et protocoles des unités fonctionnelles.

Programme de reprise après sinistre

Le Programme de reprise après sinistre de la Banque, géré par le Bureau du chef de la sécurité de l'information conformément à la Politique de gestion de la continuité des opérations et de gestion des crises et des incidents, comprend une gamme complète de procédures et de stratégies techniques visant à réduire au minimum les répercussions d'une interruption technique, à favoriser la résilience et à faciliter le retour à la normale des activités et de la prestation de services.

Le Programme encadre 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 renforcés, et des solutions de reprise spécialisées sont en place dans des sites de reprise appartenant à la Banque.

Les plans de reprise des activités après sinistre sont examinés et testés à une fréquence correspondant au risque lié à la reprise des activités, puis consignés dans des rapports internes confidentiels.

Conformité aux règlements

Le programme Gestion de la continuité des opérations et gestion des crises et des incidents de la Banque est conçu pour répondre aux exigences de différents organismes gouvernementaux, de réglementation et de surveillance, ainsi qu'aux 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, l'Authority for the Financial Markets des Pays-Bas, la Hong Kong Monetary Authority (HKMA) et la Monetary Authority of Singapore (MAS). Le Programme Gestion de la continuité des opérations et gestion des crises et des incidents de la Banque répond également à des normes internationales, dont la norme ISO 22301.

Conclusion

Les plans de continuité des opérations, les protocoles de gestion des crises et des incidents et les plans de reprise après sinistre de la Banque sont documentés, soumis à des exercices et testés, et les résultats[1] sont vérifiés de façon indépendante sur une base régulière. Les plans 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'est pas assujettie à un audit périodique en vertu de la norme SSAE 18; cependant, aux termes 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 dans les états financiers consolidés de la Banque.

Nous voulons déployer des efforts commercialement prudents et raisonnables en vue d'assurer la continuité des opérations pour la Banque et ses clients. Par contre, rien ne garantit que les systèmes de la Banque ne seront pas touchés par certains événements. Le présent document se veut un guide sur les programmes de Gestion de la continuité des opérations et gestion des crises et des incidents 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 faites par la Banque de ses opérations et de ses fournisseurs ne sont pas rendues publiques.