Guide de gestion de crise et de continuité des activités

Table des matières

Introduction

KPMG peut soutenir votre organisation :

Crisis Management Program

KPMG conçoit et réalise une série de simulations de cyberattaques indépendantes, lesquelles servent à tester les plans d'intervention d'une organisation en cas de cyberincident, ainsi que les procédures de gestion de crise de l'entreprise et du conseil d'administration en cas de perturbation informatique.

Continuité des activités

KPMG conçoit et fournit des services intégrés de continuité des activités, de reprise informatique après sinistre et de résilience, lesquels comprennent une évaluation ciblée des capacités existantes en vue de guider les plans d'amélioration.

Programme de gestion de crise

Qu'est-ce que la gestion de crise?

Dans un environnement commercial de plus en plus instable, les organisations doivent non seulement se **préparer** aux crises, mais s'y **attendre**. La capacité d'une organisation de détecter les incidents et les crises au fur et à mesure qu'ils surviennent, mais aussi d'y **réagir efficacement et de s'en remettre** fait l'objet d'une surveillance accrue.

Le cadre de gestion de crise d'une organisation est la structure qui permet l'**escalade**, la **communication** et la **coordination** en cas de crise. Il prévoit aussi la formation et la préparation des parties prenantes ayant des responsabilités en matière de gestion de crise. Les exercices sont fondés sur des scénarios axés sur les risques et simulent les pressions exercées sur les gens et les organisations ainsi que leurs attentes en période de crise.

Élaboration d'un programme de gestion de crise

Un programme de gestion de crise permet à une organisation de faire ce qui suit :

- Concevoir une série de **simulations de** cyberattaques indépendantes afin de tester ses plans d'intervention en cas de cyberincident, ainsi que les procédures de gestion de crise de l'entreprise et du conseil d'administration en cas d'attaque ciblée.
- Mettre au point une capacité d'exercice comprenant une **structure de gouvernance** et des processus connexes afin de tester périodiquement son plan d'intervention en cas de cyberincident.
- Concevoir des **mécanismes de rapport adaptés** pour l'entreprise et le conseil.
- Tester les capacités de réponse et de récupération dans **plusieurs secteurs de service et régions géographiques** en effectuant plusieurs exercices au cours d'un nombre de mois donné.

Avantages d'un programme de gestion de crise

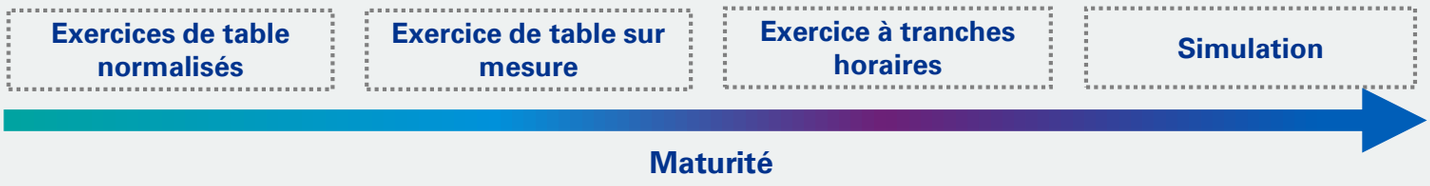
- Valider l'efficacité des stratégies de réponse dans un **environnement sûr et simulé.**
- **Renforcer les capacités** des personnes qui sont censées réagir à une crise.
- **Donner aux parties prenantes** les moyens de savoir quand agir et comment agir en cas de crise.
- Accroître la **confiance** envers la capacité de réagir à un certain nombre de crises différentes.
- Obtenir une meilleure **visibilité des risques** et des mesures d'atténuation prises.
- **Recenser** les lacunes dans les processus opérationnels avant qu'il ne soit trop tard.

Pourquoi en avez-vous besoin?

- Sans une réponse coordonnée et testée à fond à une cybercrise, aucune organisation ne peut être sûre de ses projections futures, puisqu'une entreprise, de par nature, **est constamment exposée à des cybermenaces.**
- Avec sa grande variété d'exercices, KPMG est parfaitement placé pour préparer une organisation au pire, mais aussi pour **rassurer les actionnaires et les employés** que l'organisation est suffisamment préparée à atténuer les sanctions réglementaires les plus sévères.
- Les résultats d'un programme de gestion de crise peuvent servir de guide pour l'**élaboration de stratégies futures** afin d'aider une **organisation à se protéger** contre les cyberrrisques, à se défendre contre les attaques et à en limiter la gravité, et à assurer sa survie continue malgré la perturbation des processus opérationnels essentiels.

Exercice de gestion de crise — Maturité

Le format d'exercice approprié dépend de votre maturité, comme indiqué ci-dessous.



L'approche de KPMG

Phase 0 : Mobilisation

- Demander la documentation pertinente sur la gestion de crise, par exemple le plan d'intervention en cas d'incident.
- Identifier les principaux intervenants à l'appui de l'élaboration du scénario. Par exemple, un responsable de programme et divers experts techniques.

Phase 1 : Préparation de l'exercice

- Commencer la réunion pour convenir de l'étendue et des objectifs de l'exercice.
- Comprendre les processus visés et les vulnérabilités associées dans le domaine d'activité.
- Discuter des idées de scénarios initiales.

Phase 3 : Exécution de l'exercice

- KPMG organisera un exercice de simulation pour tester les équipes requises.
- Tenir une séance de compte rendu sur la performance des participants.

Phase 2 : Conception de l'exercice

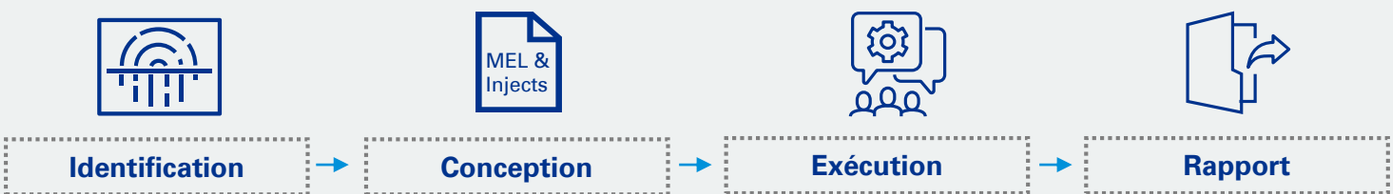
- Organiser des ateliers avec les PME pour élaborer et approuver le scénario final.
- Produire une liste chronologique des événements (LCE) et des intrants en appui au scénario.
- Effectuer un essai à blanc de la LCE et des intrants créés.
- Finaliser la liste de participants et la logistique.

Phase 4 : Rapports sur l'exercice

- Sommaire, y compris les mesures correctives générales.
- Rapport détaillé décrivant les points forts et les points faibles des activités d'intervention et de rétablissement.
- Rendre compte des résultats et des conclusions aux principaux intervenants.

Outil 4Di Simulator

- **Solution innovante et polyvalente** qui enrichit les environnements de formation pour offrir des simulations de crise immersives, stimulantes et réalistes.
- La **plateforme mobile fonctionne** sur **téléphones intelligents, tablettes** et **ordinateurs portables** et peut être utilisée n'importe où dans le monde avec une connexion Internet, que ce soit sur un même site ou dans plusieurs endroits.
- **L'outil** est utilisé pour **ajouter des intrants, enregistrer toutes les mesures prises** et faciliter les communications entre les équipes.
- Les **participants devraient consigner toutes les décisions** et les mesures prises dans l'outil pour s'assurer que leurs réponses à la simulation peuvent être évaluées de façon approfondie.



- Principales parties prenantes
- Principaux risques

- Scénario grave mais plausible
- LCE et intrants

- Exercice interactif selon la maturité

- Principales constatations
- Recommandations

Continuité des activités

Qu'est-ce que la continuité des activités?

La continuité des activités est la capacité d'une organisation à **protéger et à maintenir des processus opérationnels essentiels** en cas de perturbation. Une **gestion efficace de la continuité des activ**ités fait en sorte que les entreprises peuvent prévenir diverses perturbations opérationnelles, y réagir et s'en remettre.

Pourquoi les organisations en ont-elles besoin?

Les coûts de l'inactivité peuvent être **importants** pour les entreprises. Elles peuvent subir non seulement des dommages **financiers**, mais aussi des dommages à leur **réputation** et à leur **fonctionnement**. Par exemple, la perte, les dommages ou le refus d'accès aux services informatiques clés peuvent entraîner des retards dans les services clés offerts par une organisation.

Les entreprises ont besoin d'un **programme et d'une stratégie robustes** pour rétablir les services informatiques et les opérations de l'entreprise critiques en cas de défaillance catastrophique.

Les organisations résilientes sont mieux à même de résister aux chocs, de **protéger la valeur actionnariale** et de gérer les changements perturbateurs.

Nous aidons les organisations à **prévenir, détecter, résister et réagir** aux incidents qui menacent de compromettre la sécurité de leur personnel ou la continuité de leurs processus critiques.

Avantages d'un programme de gestion de crise

Accroissement de la résilience et des chances de survie suite à la perturbation.

Meilleure connaissance des **processus opérationnels critiques.**

La **capacité de rester opérationnel** lorsque les concurrents ne le sont pas.

Démontre **l'engagement de la direction et la confiance qu'elle inspire** aux employés et aux clients.

Permet la **visibilité des risques** et s'intègre à la gestion plus large des risques de l'entreprise.

Conformité juridique, réglementaire et fournisseur (le cas échéant).

Comment y parvenir?

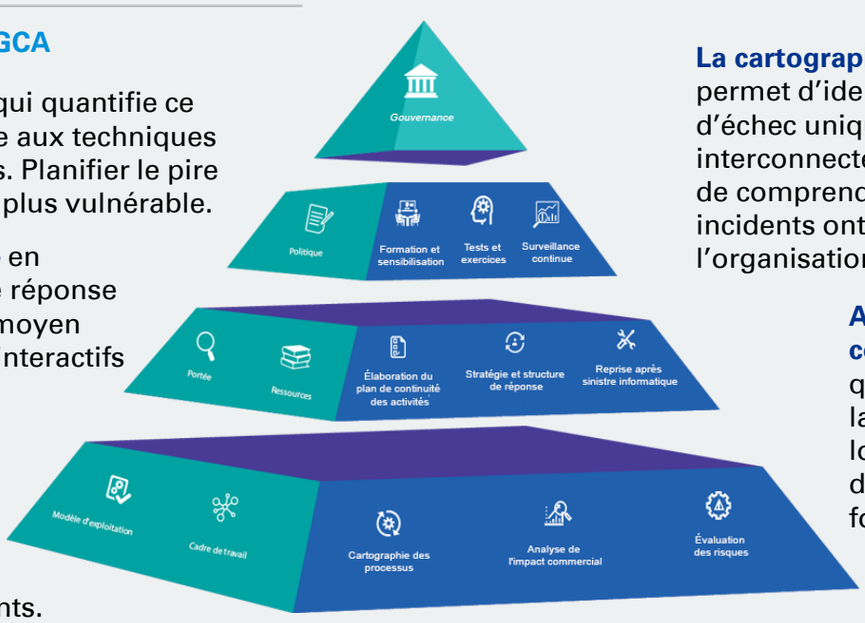
Notre équipe élaborera une trousse d'outils qui pourra être appliquée à l'ensemble d'une organisation pour atteindre l'état de maturité souhaité. Les éléments qui s'alignent sur la norme ISO22301, les lignes directrices sur les bonnes pratiques et ceux qui conviennent le mieux à la situation unique de l'organisation seront choisis. La pyramide ci-dessous met en évidence les éléments fondamentaux d'un exemple de trousse de gestion de la continuité des activités.

Éléments d'une bonne GCA

Évaluation des risques qui quantifie ce qui compte le plus grâce aux techniques d'évaluation des risques. Planifier le pire et protéger ce qui est le plus vulnérable.

Tester et faire l'exercice en mettant les capacités de réponse à l'incident à l'essai au moyen d'exercices en direct et interactifs de simulation en table.

Plans de continuité des activités (PCA) fournissant aux sites et aux fonctions un plan de continuité des activités pour les incidents.



La cartographie des processus permet d'identifier les points d'échec uniques, la nature interconnectée des processus et de comprendre comment les incidents ont un impact global sur l'organisation.

Analyse d'impact commercial (AIC) quantifiant l'impact après la perte de personnel, de locaux, de technologies, d'équipements et de fournisseurs clés.

L'approche de KPMG

Phase 1 : Exercice de découverte

Évaluation de l'état actuel — Examiner l'état actuel de la GCA par des **séances avec les intervenants**, un **examen des documents**, le production d'un **sommaire exécutif général** présentant les principales lacunes et les principales conclusions.

Atelier sur l'état cible de la GCA — Portant sur les **perspectives de l'industrie** et établissant la **maturité de l'état cible.**

Phase 2 : Conception d'une trousse

Concevoir une **trousse GCA alignée sur les normes ISO22301, les bonnes pratiques de l'industrie** et la taille, l'échelle, la culture et la complexité de votre organisation. La trousse sera conçue en tenant compte des structures de gouvernance existantes et s'adaptera aux pratiques existantes.

Phase 3 : Mise en œuvre du projet pilote facultatif

KPMG doit mener une **mise en œuvre pilote** de la stratégie, **améliorer les compétences des parties prenantes** concernées et les préparer à poursuivre l'utilisation du plan de projet.

Phase 4 : Plan de projet de mise en œuvre

Élaborer un **plan de mise en œuvre prioritaire** pour atteindre l'état cible souhaité pour la continuité des activités.

Phase 5 : Compte rendu et révision

Tenir une **séance de compte rendu** avec les parties prenantes concernées afin de résumer les conclusions et de fournir un **examen détaillé**, y compris des recommandations visant à améliorer encore la maturité.

« Notre équipe de sécurité et de gestion des risques travaille avec KPMG depuis plus de trois ans maintenant. Nous comptons sur eux pour atteindre des normes élevées et respecter des délais exigeants.

Ils font constamment preuve d'une bonne compréhension de notre entreprise et s'intègrent bien à nos équipes. »

Découverte	Conception	Mise en œuvre	Compte rendu et révision
– État actuel de la GCA – Examen des documents – Aperçu de l'industrie	– Concevoir une trousse GCA alignée sur la norme ISO22301, adaptée aux pratiques existantes	– Mise en œuvre pilote facultative – Plan de mise en œuvre complet pour obtenir des résultats	– Résumer les résultats – Examen détaillé – Recommandations

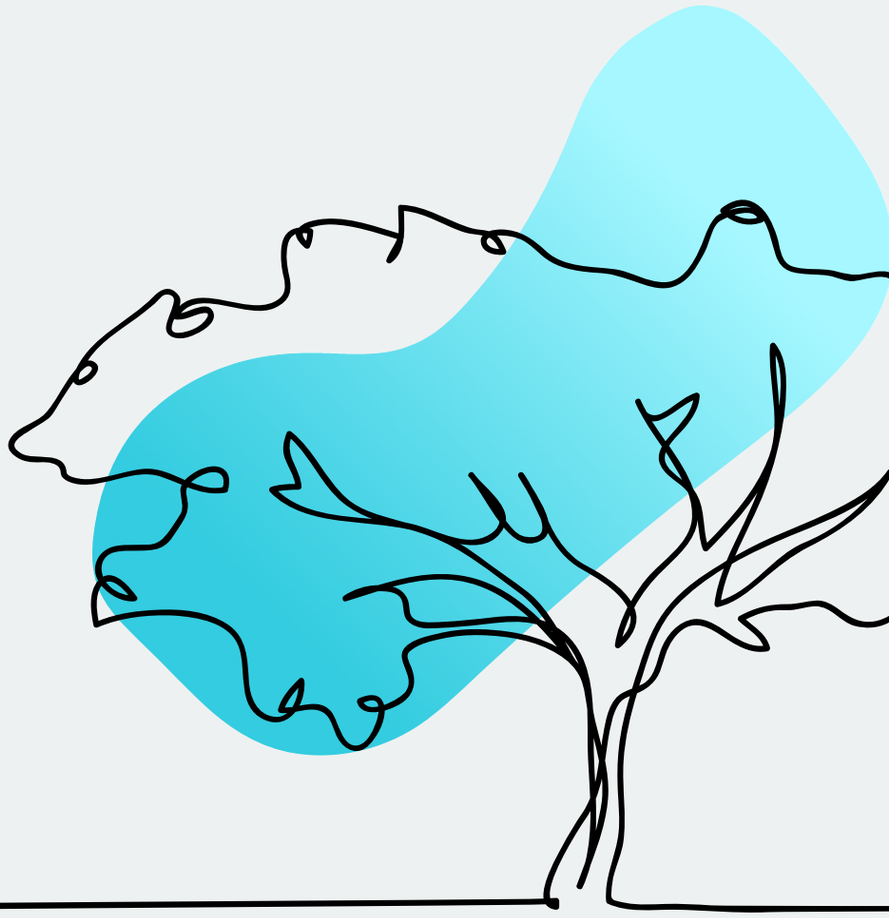
Communiquez avec nous

Doron Telem
Leader national, Services-conseils – Gestion des risques
416-777-3815
dorontelem@kpmg.ca

Kareem Sadek
Associé, Services-conseils – Gestion des risques
416-777-3446
ksadek@kpmg.ca

Hartaj Nijjar
Associé, Services-conseils – Gestion des risques
416-228-7007
hnijjar@kpmg.ca

Dave Knott
Directeur principal, Services-conseils – Gestion des risques
416-777-8654
dknott@kpmg.ca



kpmg.ca/fr