Les Pratiques Professionnelles pour la Gestion de Continuité des Activités

Ce document est maintenu par DRI International.
Pour toute question concernant ce document, veuillez communiquer avec driinfo@drii.org.
Pour plus d'informations, visitez www.drii.org.

Versie april 2023

DRI International

Table des matières

Avant-propos

À propos des Pratiques Professionnelles pour la Gestion de la Continuité des Activités

Créé et maintenu par Disaster Recovery Institute International, *Les Pratiques Professionnelles pour la Gestion de la Continuité des Activités* est un ensemble de connaissances conçu pour aider à l'élaboration, à la mise en œuvre, et le maintien d'un programme de gestion de la continuité des activités. Il est également destiné à servir d'outil pour effectuer des évaluations des programmes existants.

L'utilisation du cadre de Pratique Professionnelle pour développer, mettre en œuvre, maintenir un programme de continuité des activités peut réduire la probabilité d'importantes lacunes dans un programme et peut augmenter la cohésion du programme. L'utilisation des Pratiques Professionnelles pour évaluer un programme peut permettre d'identifier les lacunes ou les faiblesses afin qu'elles puissent être corrigées.

La gestion de la continuité des activités (GCA) est un processus de gestion holistique qui identifie les menaces pour une organisation et les impacts sur les opérations commerciales que ces menaces, si elles se concrétisent, pourraient causer, et qui fournit un cadre pour renforcer la résilience organisationnelle avec la capacité d'une réponse efficace qui protège les intérêts de ses principales parties prenantes, sa réputation, sa marque et ses activités créatrices de valeur. Les termes sont définis dans le *Glossaire International pour la Résilience* publié et maintenu par DRI International.

DRI rend disponibles à la fois *Les Pratiques Professionnelles pour la Gestion de la Continuité des Activités* et le *Glossaire International pour la Résilience* en téléchargement gratuit via drii.org. Les deux documents sont disponibles en plusieurs langues.

Note sur la version actuelle

Dans le cadre des efforts continus de DRI International pour maintenir la pertinence et l'utilité des Pratiques Professionnelles, une révision approfondie du fond, de la forme et de la fonction a été entreprise à compter du 1er novembre 2021 et jusqu'au 1er août 2022. Les objectifs étaient de fournir de l'information qui comprendrait :

- Une version améliorée de la Pratique Professionnelle 5 : Préparation et interventions d'urgence afin d'inclure davantage d'activités de préparation liées à la gestion des incidents ;
- Plus d'information sur l'identification des diverses cybermenaces et stratégies de remédiation en intégrant les activités de cybersécurité à la gestion de la continuité des activités ;
- Renforcer l'utilisation de l'assurance comme outil de transfert des risques et fournir des types de polices d'assurance plus spécifiques qui devraient faire partie intégrante de la gestion de la continuité des activités ;
- Introduction de techniques de sauvegarde de données plus robustes ;
- Des stratégies plus spécifiques à la technologie ;
- Plus de stratégies de fabrication.

De plus, les titres de quatre des pratiques professionnelles ont été modifiés :

- La pratique professionnelle 1 est passée de « Démarrage et gestion du programme » à « Gestion du programme » ;
- La pratique professionnelle 5 est passée de « Interventions d'urgence » à « Préparation et interventions d'urgence » afin de mettre l'accent sur les activités nécessaires à l'élaboration d'un plan d'intervention efficace ;
- La pratique professionnelle 8 est passée de « Exercice, évaluation et maintenance du plan de continuité des activités » à « Exercice / test, évaluation et maintenance du plan de continuité des activités » par souci d'uniformité ; et
- La pratique professionnelle 10 est passée de « Coordination avec les agences externes » à « Coordination avec les agences et ressources externes ».

Sauf indication contraire, les listes ne sont pas présentées dans un ordre particulier. Les besoins peuvent varier d'une entité à l'autre.

Depuis la dernière révision des pratiques professionnelles, la discipline de la résilience s'est développée pour devenir plus holistique et inclusive, tout comme le vocabulaire technique et commercial. À la prochaine étape de la mise à jour du processus des pratiques professionnelles, DRI réconciliera la terminologie utilisée dans les pratiques professionnelles et celle utilisée dans *le Glossaire International de la Résilience.* L'objectif est d'ajouter et de modifier des termes dans le glossaire pour refléter l'évolution du langage.

Remerciements

Merci aux Membres de notre Comité de Pratique Professionnelle pour leur contribution à la profession.

Comité de révision
Président, Raymond Seid, MBCP, CBLA, ARMP
Coordonnatrice de l'IRN, Al Berman, MBCP, CBCLA, CCRP
Michele Turner, MBCP
Andrea Abrams, PCCS
Mike Semel, CBCP

Comité d'évaluation
Don Schmidt, CBCP, CBCLA

Éditeurs
Chloe Demrovsky, CBCV
Buffy Rojas Leach

Traduction française
Réjean Pesant, CBCP

Sommaire

Objectifs des Pratiques professionnelles pour la gestion de la continuité des activités

1. **Gestion du programme**
   1.1. Établir la nécessité d'un programme de continuité des activités.
   1.2. Introduire des concepts clés, tels que la gestion du programme, la sensibilisation aux risques, l'impact sur les fonctions et processus critiques, les stratégies de rétablissement, la formation et la sensibilisation, ainsi que les exercices / tests.
2. **Évaluation des risques**
   2.1. Identifiez les risques susceptibles d'avoir un impact sur les ressources, les processus ou la réputation d'une entité.
   2.2. Évaluer les risques pour déterminer les impacts négatifs potentiels sur l'entité, permettant à l'entité de déterminer les moyens les plus efficaces de les réduire.
3. **Bilan des impacts d'affaires**
   3.1. Identifier et prioriser toutes les fonctions, processus et dépendances de l'entité afin de déterminer le plus grand impact sur l'entité si les fonctions ne sont pas disponibles. Cette analyse doit être conservée et disponible pour aider l'entité à comprendre les incidents et/ou les conséquences qui en découlent. Quantifier l'impact sur l'entité, ses services et les parties affectées.
   3.2. Analyser, documenter et communiquer les résultats pour mettre en évidence tous les écarts entre les exigences de l'entité et ses capacités actuelles.
4. **Stratégies de continuité des activités**
   4.1. Choisir des stratégies pour réduire les écarts identifiés lors de l'évaluation des risques et du bilan des impacts d'affaires.
   4.2. Identifier les principales fonctions de l'entité, y compris les fournisseurs de services tiers potentiels, avec le soutien de la partie responsable du bilan des impacts d'affaires.
5. **Préparation et interventions d'urgence**
   5.1. Comprendre les types d'incidents qui pourraient menacer la vie, les biens, les opérations ou l'environnement et leurs impacts potentiels.
   5.2. Établir et maintenir des capacités pour protéger la vie, les biens, les opérations et l'environnement contre les incidents potentiels grâce à la mise en œuvre d'un système de gestion des incidents pour commander, contrôler et coordonner les activités d'intervention, de continuité et de rétablissement avec des ressources internes et externes.
6. **Élaboration et mise en œuvre du plan**
   6.1. Documenter les plans à être utilisé lors d'un incident qui permettra à l'entité de continuer à fonctionner.
   6.2. Définir les critères d'exercice / test pour vérifier que les plans permettront d'atteindre l'objectif souhaité.
7. **Programmes de sensibilisation et de formation**
   7.1. Établir et maintenir des programmes de formation et de sensibilisation qui permettent au personnel de répondre aux incidents perturbateurs de manière calme et efficace.
8. **Exercice/test, évaluation et maintenance du plan de continuité des activités**
   8.1. Établir un plan d'exercice/test de continuité des activités, d'évaluation, et de programme de maintenance afin d'améliorer l'état de préparation de l'entité.
9. **Communication de crise**
   9.1. Créer et maintenir un plan de communication de crise.
   9.2. Veiller à ce que le plan de communication de crise permette une communication rapide et efficace avec les parties internes et externes.
10. **Coordination avec les agences et ressources externes**
    10.1. Établir des politiques et des procédures pour coordonner les activités d'intervention avec les entités publiques et les ressources privées applicables, conformément à la pratique professionnelle cinq : Préparation et interventions d'urgence.

Pratique professionnelle 1: Gestion du programme

Objectifs

1. Établir la nécessité d'un programme de continuité des activités.
2. Introduire des concepts clés, tels que la gestion du programme, la sensibilisation aux risques, l'impact sur les fonctions et processus critiques, les stratégies de rétablissement, la formation et la sensibilisation, ainsi que les exercices / tests.

Rôle du professionnel

1. Déterminer les besoins d'un programme de la continuité des activités.
2. Obtenir le soutien et le financement du programme de continuité des activités. Créer de la documentation pour faciliter l'adoption du programme de leadership et le soutien continu.
3. Coordonner et/ou diriger la mise en œuvre du programme de continuité des activités dans l'ensemble de l'entité.

Activités

1. Déterminer les besoins d'un programme de la continuité des activités.
    1.1. Rechercher, référencer et quantifier les exigences et restrictions commerciales, légales, réglementaires et contractuelles pertinentes, tant d'un point de vue interne qu'externe. Fournir des recommandations sur le respect et la conformité pour l'entité. Demander à des experts en la matière de fournir des informations détaillées sur les considérations opérationnelles et techniques spécifiques qui s'appliquent à l'entité. Faire référence aux normes pertinentes.
    1.2. Identifier et résoudre tout conflit entre la gouvernance, les politiques, les procédures et les exigences externes de l'entité. S'assurer que le programme de continuité des activités proposé comble adéquatement toute lacune qui réduirait l'efficacité du programme. Passez en revue les directives, les incidents antérieurs et tous les rapports d'audit existants.
    1.3. Énoncer les avantages de la continuité des activités dans le contexte de la mission de l'entité.
    1.4. Expliquer le rôle du leadership, y compris l'imputabilité et la responsabilité liées à un programme de continuité des activités inefficace.
    1.5. Élaborer des rapports et des présentations formels visant à accroître la sensibilisation à l'impact potentiel des risques pour l'entité.
2. Obtenir le soutien et le financement du programme de continuité des activités. Créer de la documentation pour faciliter l'adoption du programme de leadership et le soutien continu.
    2.1. Élaborer une charte pour le programme de continuité des activités dans le contexte de la mission de l'entité. Inclure les objectifs, les hypothèses et la portée du programme de continuité des activités.
    2.2. Élaborer un budget et acquérir des ressources pour le programme de continuité des activités.
    2.3. Définir la structure du programme de continuité des activités. Identifier les besoins potentiels en matière de politique et les facteurs critiques de succès.
    2.4. Identifier le leadership pour l'élaboration de programmes de continuité des activités.
    2.5. Présenter la structure proposée pour le programme de continuité des activités afin d'obtenir le soutien et l'approbation de la direction pour le programme de continuité des activités.
    2.6. Obtenir l'approbation de la direction pour le budget.
    2.7. Mettre sur pied un comité directeur ou un organisme de surveillance qui sera responsable du programme de continuité des opérations.
    2.8. Définir l'étendue des responsabilités et de l'imputabilité globales de chaque membre du comité directeur/organe de surveillance et de ses fonctions de soutien.

3. Coordonner et/ou diriger la mise en œuvre du programme de continuité des activités dans l'ensemble de l'entité.
   - 3.1. Conseiller le comité directeur ou l'organisme de surveillance pour diriger la mise en œuvre des objectifs, de la structure du programme et des facteurs critiques de succès. Assurer l'harmonisation avec les politiques organisationnelles existantes.
   - 3.2. Élaborer des politiques, normes et procédures pour le programme de la continuité des activités dans le contexte de la mission, les objectifs et les activités de l'entité.
   - 3.3. Établir le but et obtenir les ressources nécessaires au programme de la continuité des activités.
   - 3.4. Identifier les équipes pour la mise en œuvre du programme de la continuité des activités, incluant les équipes qui participeront à la réalisation des activités suivantes:
     - 3.4.1. Évaluation des risques et des stratégies
     - 3.4.2. Bilan des impacts d'affaires
     - 3.4.3. Sélection et mise en œuvre des stratégies de rétablissement
     - 3.4.4. Gestion, intervention et rétablissement des incidents
     - 3.4.5. Gestion de crise et communication
     - 3.4.6. Analyse des lacunes post-incident et mise en œuvre gagnée
     - 3.4.7. Documentation des plans de continuité des activités
     - 3.4.8. Planifier les activités d'exercice/test, de maintenance et d'audit
     - 3.4.9. Activités reliées aux interventions immédiates, au rétablissement et à la restauration durant/après un événement.
   - 3.5. Assurer le suivi de l'évolution budgétaire du programme de la continuité des activités selon les processus de gestion budgétaires existants.
   - 3.6. Élaborer les plans de projet pour les principales composantes tels que l'évaluation des risques et processus du bilan des impacts d'affaires et identifier les activités requises pour soutenir les facteurs clés de succès convenus, incluants :
     - 3.6.1. Le calendrier d'implantation
     - 3.6.2. L'estimation des efforts
     - 3.6.3. Les jalons
     - 3.6.4. Les besoins en personnel.
   - 3.7. Superviser l'efficacité générale du programme de continuité des activités.
     - 3.7.1. Élaborer, surveiller, suivre et rendre compte des exigences continues en matière de gestion et de documentation pour le programme de continuité des activités.
     - 3.7.2. Surveiller, suivre et rendre compte de la conformité / le respect aux normes réglementaires et de l'industrie.
     - 3.7.3. Élaborer et exécuter des stratégies d'analyse comparative internes et externes.
   - 3.8. Informez la direction à mesure que les circonstances changent.
     - 3.8.1. Élaborer un calendrier pour rendre compte de l'état du programme de continuité des activités à la direction générale de l'entité.
     - 3.8.2. Élaborer des rapports pour la direction générale contenant une information précise et ponctuelle sur les éléments clés du programme de la continuité des activités.

Pratique professionnelle 2: Évaluation des risques

Objectifs

1. Identifiez les risques susceptibles d'avoir un impact sur les ressources, les processus ou la réputation d'une entité.
2. Évaluer les risques pour déterminer les impacts négatifs potentiels sur l'entité, permettant à l'entité de déterminer les moyens les plus efficaces de les réduire.

Rôle du professionnel

1. Travailler avec la direction et tout groupe de gestion des risques pour obtenir un accord sur une méthodologie d'évaluation des risques.
2. Identifier, élaborer et mettre en œuvre les activités de collecte d'information à travers l'entité pour identifier les risques.
3. Déterminer la probabilité et les impacts des risques identifiés.
4. Évaluer l'impact des risques sur les facteurs essentiels à la conduite des activités de l'entité.
5. Identifier et évaluer l'efficacité des contrôles utilisés pour réduire l'impact des expositions.
6. Documenter et présenter l'évaluation des risques et vulnérabilités et les recommandations à la direction pour approbation.
7. Demander l'approbation de la direction pour développer la propension au risque de l'entité, à utiliser comme base à la gestion d'un processus continu d'évaluation des risques.

Activités

1. Travailler avec la direction et tout groupe de gestion des risques pour obtenir un accord sur une méthodologie d'évaluation des risques.
    1.1. Travailler avec la direction et les groupes de gestion des risques pour déterminer les besoins internes et externes.
    1.2. Obtenir un accord sur une méthode d'évaluation des risques claire et normalisée.
    1.3. Comprendre le seuil et la propension au risque de l'entité.
    1.4. Identifier les méthodologies et les outils d'analyse des risques, qui peuvent inclure, sans s'y limiter, des analyses quantitatives et qualitatives.
    1.5. Examiner et intégrer les facteurs de fiabilité et de confiance des données utilisées.
    1.6. Choisir la méthodologie et les outils appropriés pour la mise en œuvre à l'échelle de l'entité.
    1.7. Établir les critères de mesures nécessaires pour quantifier la probabilité et l'impact des risques identifiés ainsi que l'efficacité de tous contrôles existants.
2. Identifier, élaborer et mettre en œuvre les activités de collecte d'information à travers l'entité pour identifier les risques.
    2.1. Identifier la méthodologie à utiliser pour le processus de collecte d'informations.
    2.2. Collaborer avec les groupes pertinents de l'entité, y compris, mais sans s'y limiter, à la gestion des risques, les conseillers juridiques, les responsables de la sécurité physique et la sécurité de l'information et les parties prenantes concernées pour identifier les risques.
    2.3. Déterminer les sources d'information qui seront utilisées pour recueillir les données sur les risques et référencer ces sources dans le rapport. Élaborer une stratégie de collecte des informations conforme aux politiques de l'entité.
    2.4. Concevoir des méthodes de collecte de l'information et de distribution à l'échelle de l'entité, y compris, mais sans s'y limiter, des formulaires, des questionnaires, des entretiens, des réunions et/ou des combinaisons de ces processus.
    2.5. Identifier les risques de l'entité.
        2.5.1. Obtenir une vue globale des risques à l'échelle de l'entité en identifiant les risques, en tenant compte de la fréquence, la probabilité, la vitesse de propagation, de la sévérité et de l'impact financier et/ou sur la réputation
        2.5.2. Identifier les sources d'exposition aux risques tant de l'interne que de l'externe, qui peuvent inclure, sans s'y limiter, les phénomènes naturels, les expositions technologiques, et les actes humains; les expositions de l'industrie ou d'un modèle d'affaires; les actes accidentels et intentionnels; les expositions ou les risques contrôlables, ainsi que ceux qui sont hors du contrôle de l'entité; et les incidents avec et sans avertissement préalable.

3. Déterminer la probabilité et les impacts des risques identifiés.
    3.1. Développer une méthode pour évaluer les expositions et les risques en termes de fréquence, de probabilité, de taux de développement, de gravité, d'impact, et d'existence d'avertissements préalables à l'incident comme dans le cas des ouragans/typhons/cyclones.
    3.2. Identifier les impacts des risques identifiés par catégorie, qui peuvent inclure, sans s'y limiter, la disponibilité de la main-d'œuvre, la chaîne d'approvisionnement, la cybersécurité, les technologies de l'information, la livraison de produits ou de services, les installations, la réputation, les aspects juridiques et réglementaires.
    3.3. Évaluer les risques identifiés en fonction des risques qui sont sous le contrôle de l'entité et de ceux qui sont hors de son contrôle.
4. Évaluer l'impact des risques sur les facteurs essentiels à la conduite des activités de l'entité.
    4.1. Fournir le personnel, les technologies de l'information, les technologies de communication et la logistique, comme le transport. Identifier et évaluer l'efficacité des contrôles et des sauvegardes actuellement en place.
    4.2. Identifier et évaluer l'efficacité de la protection des actifs. Identifier et évaluer l'efficacité des contrôles et des protections actuellement en place pour les groupes internes et externes dont l'entité dépend pour mener ses opérations.
    4.3. Identifier et évaluer l'efficacité des mesures prises pour réduire la probabilité d'occurrence d'incidents susceptibles de nuire à la capacité de mener des activités, ce qui peut inclure, sans s'y limiter, l'emplacement des installations, les politiques et procédures de sécurité, la formation sur l'utilisation appropriée des équipements et outillages et maintenance préventive.
    4.4. Identifier et évaluer l'efficacité des contrôles existants pour atténuer les expositions aux impacts tels que les contrôles préventifs, qui peuvent inclure, mais sans s'y limiter, la santé et la sécurité du personnel, les pratiques de sécurité physique, la sécurité de l'information, les pratiques d'emploi et les pratiques de confidentialité.
5. Identifier et évaluer l'efficacité des contrôles utilisés pour réduire l'impact des expositions.
    5.1. Évaluer les équipements qui peut inclure, mais sans s'y limiter, les systèmes de gicleurs, des brigades de pompiers, des génératrices, des connexions Internet multiples, des sauvegardes de données et des systèmes d'alimentation sans coupure (UPS).
    5.2. Évaluer les communications liées à la sécurité au sein de l'entité et avec les fournisseurs de services externes
    5.3. Identifier les éléments déclencheurs pour les services clés et les secteurs de soutien afin d'identifier, d'escalader et d'exécuter les stratégies choisies afin d'adresser les risques.
    5.4. Recommander les changements nécessaires pour réduire l'impact des risques identifiés, qui peuvent inclure, mais sans s'y limiter :
        5.4.1. Identifier les changements apportés à la protection physique, y compris, mais sans s'y limiter, les actions suivantes :
            5.4.1.1. Identifier les exigences nécessaires pour restreindre l'accès à toutes les zones contrôlées.
            5.4.1.2. Étudier la nécessité d'installer des barrières, de renforcer les structures et d'installer des alarmes pour dissuader les entrées dangereuses et/ou non autorisées. Abordez les vulnérabilités de l'emplacement qui peuvent résulter de la santé, de la construction physique, de l'emplacement géographique, des entreprises voisines, de l'infrastructure des installations et de l'infrastructure de la communauté. Identifier la nécessité d'utiliser du personnel qualifié et/ou des équipements pour effectuer des contrôles aux points d'entrée. Évaluer le besoin d'équipement de surveillance aux points de contrôle d'accès.
            5.4.1.3. Identifier les modifications apportées à la sécurité et les contrôles d'accès, à la couverture d'assurance des locataires et les baux de location.
        5.4.2. Identifier les changements en matière de cybersécurité et de technologie de l'information, y compris, mais sans s'y limiter, les actions suivantes:
            5.4.2.1. Évaluez la nécessité de protéger les données stockées, qu'elles soient utilisées pour le traitement ou pour une sauvegarde en cours. Étudier des techniques telles que l'air gapping et l'isolement pour protéger les données de sauvegarde.
            5.4.2.2. Évaluer la sécurité des informations, y compris le matériel, les logiciels, les données et la surveillance du réseau, comme la détection et la notification.

5.4.2.3. Évaluer la protection de l'emplacement physique des actifs de cybersécurité et de technologie de l'information.
5.4.3. Identifier les changements dans les politiques, les procédures, la communication et les procédures de formation du personnel.
5.4.4. Utiliser une liste de contrôle et faire réviser le travail avant la mise en œuvre.
5.4.5. Identifier les changements, y compris la duplication et les redondances intégrées aux services publics.
5.5. Interagir avec les ressources externes, qui peuvent inclure, sans s'y limiter, les vendeurs, les fournisseurs et les sous-traitants.

6. Documenter et présenter l'évaluation des risques et vulnérabilités et les recommandations à la direction pour approbation.
   6.1. Préparer un rapport d'évaluation des risques normalisant l'analyse à l'échelle de l'entité.
   6.2. Documenter et présenter les résultats de l'évaluation des risques, qui peuvent inclure, sans s'y limiter, les éléments suivants:
      6.2.1. Informations sur les risques et les expositions basées sur l'analyse des risques et des vulnérabilités
      6.2.2. Une évaluation de tous les contrôles et/ou stratégies existants pour gérer les risques connus.
      6.2.3. Recommandations pour de nouveaux contrôles à mettre en place ; fournir une analyse coûts/bénéfices pour justifier les recommandations.
      6.2.4. Recommandations priorisées pour la mise en œuvre de tout nouveau contrôle.
      6.2.5. Recommandations concernant les moyens appropriés pour transférer le risque.
7. Demander l'approbation de la direction pour développer la propension au risque de l'entité, à utiliser comme base à la gestion d'un processus continu d'évaluation des risques.
   7.1. Documenter les décisions de report de la direction et/ou de non-acceptation des risques, le cas échéant.

Pratique professionnelle 3: Bilan des impacts d'affaires

Objectifs

1. Identifier et prioriser toutes les fonctions, processus et dépendances de l'entité afin de déterminer le plus grand impact sur l'entité si les fonctions ne sont pas disponibles. Cette analyse doit être conservée et disponible pour aider l'entité à comprendre les incidents et/ou les conséquences qui en découlent. Quantifier l'impact sur l'entité, ses services et les parties affectées.
2. Analyser, documenter et communiquer les résultats pour mettre en évidence tous les écarts entre les exigences de l'entité et ses capacités actuelles.

Rôle du professionnel

1. Identifier et documenter les critères qualitatifs et quantitatifs à utiliser pour évaluer l'impact sur l'entité résultant d'un incident.
2. Recommander les objectifs et la portée du processus du bilan des impacts d'affaires.
3. Établir les critères et la méthodologie à utiliser dans la conduite du processus du bilan des impacts d'affaires.
4. Analyser les données recueillies par rapport aux critères approuvés afin d'établir un objectif de temps de rétablissement (OTR), un objectif de point de rétablissement (OPR) et des ressources pour chaque domaine opérationnel et sa technologie de soutien.
5. Préparer et présenter les résultats du bilan des impacts d'affaires. Obtenir l'acceptation des objectifs de temps de rétablissement, des objectifs de point de rétablissement et des ressources tels que détaillés dans le bilan des impacts d'affaires.

Activités

1. Identifier et documenter les critères qualitatifs et quantitatifs à utiliser pour évaluer l'impact sur l'entité résultant d'un incident.
    1.1. Identifier les échéances critiques (par exemple, les virements électroniques, la paie ou les dépôts réglementaires).
    1.2. Définir et obtenir l'approbation des critères à utiliser pour évaluer l'impact sur l'entité et les parties concernées, qui peuvent inclure, mais sans s'y limiter, les éléments suivants :
        1.2.1. Impact sur la clientèle, y compris, mais sans s'y limiter, la rapidité avec laquelle les clients apprendront l'existence d'un problème ; la probabilité qu'ils mettent fin à leur relation avec l'entité ; exigences des accords existants et les impacts sur les accords de niveau de service (ANS) ; et impact de l'entité sur les chaînes d'approvisionnement des clients.
        1.2.2. Impacts financiers, y compris, mais sans s'y limiter, à la perte de revenus ; perte de profits ; impact sur les flux de trésorerie ; impact sur la part de marché ; impact sur le cours de l'action ; impact sur la cote de crédit ; amendes ou pénalités contractuelles ; pertes résultant des paiements requis pour les coûts fixes ; ou augmentation des dépenses liées aux heures supplémentaires.
        1.2.3. Impacts réglementaires, y compris, mais sans s'y limiter, les amendes, les pénalités, le rappel involontaire de produits ou la révocation de licences ou permis.
        1.2.4. Impacts opérationnels, y compris, mais sans s'y limiter, l'interruption ou la réduction des niveaux de service et les perturbations de la chaîne d'approvisionnement.
        1.2.5. Impacts sur la réputation, y compris, mais sans s'y limiter, l'attention négative des médias, les commentaires négatifs sur les réseaux sociaux, la perception négative de la communauté et l'impact sur la confiance des actionnaires.
        1.2.6. Impact sur la main-d'œuvre et les parties intéressées, y compris, mais sans s'y limiter, la perte de vie, les blessures, l'impact sur les services communautaires, l'environnement et l'impact psychologique.
    1.3. Éléments financiers qui assurent le transfert des risques par le biais d'une assurance, qui peuvent inclure, mais sans s'y limiter, l'interruption d'activités, l'interruption d'activités collatérales, la chaîne d'approvisionnement, la cybersécurité et l'assurance dépenses supplémentaires.

2. Recommander les objectifs et la portée du processus du bilan des impacts d'affaires.
   2.1. Obtenir l'accord de la direction à l'égard de la méthodologie de BIA et des critères à utiliser pour établir le processus et méthodologie du bilan des impacts d'affaires.
   2.2. Identifier et obtenir le soutien de la direction et/ou identifier les responsables du bilan des impacts d'affaires.
   2.3. Choisissez une méthodologie ou un outil pour le processus du bilan des impacts d'affaires et la collecte de données. Les données à collecter doivent inclure les processus opérationnels et les besoins en ressources supplémentaires en fonction de la durée de rétablissement.
   2.4. Les données à collecter doivent inclure l'impact de la perte de toute ressource nécessaire au processus opérationnel.
   2.5. Les données à collecter devraient inclure les dépendances internes et externes.
   2.6. Identifier les exigences supplémentaires spécifiques à l'entité.
   2.7. Planifier et coordonner la collecte et l'analyse des données.
   2.8. La collecte des données peut être effectuée au moyen de questionnaires.
      2.8.1. Développer les questionnaires avec les directives.
      2.8.2. Organiser des rencontres de démarrage de projet pour distribuer et expliquer les questionnaires.
      2.8.3. Assister les répondants pour remplir leur questionnaire.
   2.9. Planifier des entretiens ou des ateliers de suivi si une clarification des données fournies est nécessaire.
      2.9.1. Établir un ordre du jour et un ensemble d'objectifs.
      2.9.2. La collecte de données peut être effectuée à l'aide d'ateliers.
      2.9.3. Pour chaque atelier, identifier le niveau approprié de participants à l'atelier et obtenir l'accord de la direction et/ou identifier la partie responsable.
      2.9.4. Choisissez un lieu approprié en évaluant l'emplacement, les installations et la disponibilité des participants. Envisagez des entretiens virtuels pour les participants qui ne peuvent pas assister en personne.
      2.9.5. Animer et diriger l'atelier.
      2.9.6. S'assurer que les objectifs de l'atelier soient atteints.
      2.9.7. S'assurer d'identifier tous les points en suspens à la fin de l'atelier et de faire les suivis appropriés.
   2.10. Identifier les principales fonctions de l'entité, y compris les potentiels fournisseurs de services externes, avec le soutien de la partie responsable du bilan des impacts d'affaires.
      2.10.1. Recueillir et réviser les organigrammes existants.
      2.10.2. Identifier les membres d'équipes pour représenter chacun des domaines fonctionnels de l'entité.
      2.10.3. Identifier les représentants appropriés des fournisseurs de services externes qui participeront au processus de collecte de données.
      2.10.4. Informer les personnes sélectionnées sur le processus du bilan des impacts d'affaires et de son objectif.
   2.11. En utilisant la méthodologie choisie, réaliser la collecte des données nécessaires pour soutenir le bilan des impacts d'affaires.
3. Établir les critères et la méthodologie à utiliser dans la conduite du processus du bilan des impacts d'affaires.
   3.1. Identifier et obtenir un accord sur les méthodes d'évaluation quantitative et qualitative des impacts financiers et non financiers potentiels.
   3.2. Créer un calendrier pour effectuer le bilan des impacts d'affaires.
4. Analyser les données recueillies par rapport aux critères approuvés afin d'établir un objectif de temps de rétablissement (OTR), un objectif de point de rétablissement (OPR) et des ressources pour chaque domaine opérationnel et sa technologie de soutien.
   4.1. Analyser les données collectées pour déterminer l'ordre de priorité des processus. Documenter toutes les dépendances qui existent entre chaque processus d'affaires et les composants de soutien, y compris, mais sans s'y limiter, les systèmes de données et les technologies associées, la chaîne d'approvisionnement, les fournisseurs de services externes autres ressources. Ces dépendances peuvent être intradépartementales, interdépartementales ou impliquer des relations externes.

4.2. Déterminer l'ordre de rétablissement des fonctions d'affaires et des technologies à l'aide de l'analyse des données collectées.

5. Préparer et présenter les résultats du bilan des impacts d'affaires. Obtenir l'acceptation des objectifs de temps de rétablissement, des objectifs de point de rétablissement et des ressources tels que détaillés dans le bilan des impacts d'affaires.
   5.1. Rédiger une version préliminaire du rapport de bilan des impacts d'affaires en utilisant les résultats initiaux, en soulignant les lacunes identifiées dans une analyse des écarts.
      5.1.1. Fournir un énoncé de la mission, des buts et objectifs de l'entité.
      5.1.2. Résumer l'impact sur la mission, ces buts et objectifs de l'entité qui peut résulter d'un incident perturbateur.
      5.1.3. Fournir une liste priorisée des processus et services de l'entité, y compris les objectifs de temps de rétablissement et les objectifs de point de rétablissement, les besoins en ressources nécessaires pour rétablir et reprendre les opérations, et une analyse des écarts entre les capacités de rétablissement actuelles et les objectifs, spécifiquement:
         5.1.3.1. Temps (objectif de temps de rétablissement par rapport au temps de rétablissement réel)
         5.1.3.2. Données (objectif du point de rétablissement par rapport à la perte réelle de données)
         5.1.3.3. Ressources (besoins en ressources de rétablissement par rapport aux ressources de rétablissement réelles)
      5.1.4. Produire le rapport préliminaire à la direction pour obtenir leurs commentaires.
      5.1.5. Réviser les commentaires obtenus auprès de la direction et ajuster le rapport au besoin.
      5.1.6. Planifier des ateliers ou des réunions avec la direction pour discuter de tout problème avec les résultats initiaux.
      5.1.7. Mettre à jour les rapports pour refléter tout changement découlant des ateliers ou des réunions.
   5.2. Préparer le rapport final du bilan des impacts d'affaires et le soumettre à la direction pour approbation.
   5.3. Obtenir l'acceptation et l'approbation de la direction pour les objectifs de temps de rétablissement, les objectifs de point de rétablissement et les ressources pour chaque domaine fonctionnel, tels que définis par les conclusions du rapport final du bilan des impacts d'affaires.

Pratique professionnelle 4: Stratégies de continuité des activités

Objectifs

1. Choisir des stratégies pour réduire les écarts identifiés lors de l'évaluation des risques et du bilan des impacts d'affaires.
2. Identifier les principales fonctions de l'entité, y compris les fournisseurs de services tiers potentiels, avec le soutien de la partie responsable du bilan des impacts d'affaires.

Rôle du professionnel

1. Utiliser les données recueillies au cours des processus d'évaluation des risques et du bilan des impacts d'affaires pour identifier les stratégies de continuité et de reprise disponibles pour les activités de l'entité qui permettront d'atteindre les objectifs de temps de rétablissement et objectifs de point de rétablissement définis dans le bilan des impacts d'affaires.
2. Protéger les documents papier essentiels qui risquent d'être détruits.
3. Utiliser les données recueillies au cours de l'évaluation des risques et du bilan des impacts d'affaires pour identifier les stratégies de continuité et de reprise de la technologie de l'entité afin d'atteindre les objectifs de temps de rétablissement et objectifs de point de rétablissement définis dans le bilan des impacts d'affaires.
4. Identifier les problèmes de la chaîne d'approvisionnement (pour les fournisseurs et les clients) à partir du bilan des impacts d'affaires qui peuvent affecter la sélection de la stratégie de rétablissement.
5. Évaluer les coûts de mise en œuvre des stratégies identifiées grâce à une analyse coûts/bénéfices.
6. Recommander des stratégies et obtenir l'approbation de la direction pour leur mise en œuvre.

Activités

1. Utiliser les données recueillies au cours des processus d'évaluation des risques et du bilan des impacts d'affaires pour identifier les stratégies de continuité et de reprise disponibles pour les activités de l'entité qui permettront d'atteindre les objectifs de temps de rétablissement et objectifs de point de rétablissement définis dans le bilan des impacts d'affaires.
    1.1. Réviser les exigences de rétablissement identifiées pour chacun des domaines fonctionnels de l'entité.
    1.2. Identifier des stratégies alternatives de continuité des activités. Les options potentielles incluent, mais sans s'y limiter, les stratégies suivantes :
        1.2.1. Élaborer des solutions alternatives manuelles.
        1.2.2. Développer des ententes réciproques.
        1.2.3. Identifier des stratégies alternatives pour les installations. Identifiez les espaces internes à double usage qui pourraient être équipés pour soutenir le rétablissement, tels que les salles de conférence, les salles de formation ou les cafétérias. S'assurer que le temps nécessaire pour préparer et équiper l'espace est cohérent avec les objectifs de temps de rétablissement.
        1.2.4. Évaluer et identifier le ou les sites alternatifs externes. Examiner les options de sites alternatifs en utilisant les critères suivants : l'emplacement ; la disponibilité et la pertinence de l'espace; les capacités de communication, y compris la voix et les données ; la disponibilité de l'équipement et du matériel; et la sécurité et la robustesse du site, y compris la disponibilité des ressources.
        1.2.5. Signer une entente d'impartition ou avec un fournisseur de service externe.
        1.2.6. Transférer la charge de travail à un autre site actif.
        1.2.7. Transférer le personnel à un autre site actif.
        1.2.8. Suspendre les activités d'un site actif qui ne sont pas sensibles aux délais ou aux interruptions et y transférer le personnel / la charge de travail du site affecté au site de reprise.
        1.2.9. Construire un site alternatif dédié.
        1.2.10. Assigner le personnel au télétravail.

1.3. Différents types d'opérations peuvent avoir des besoins spécifiques. Par exemple, la fabrication/distribution peut utiliser les stratégies de rétablissement suivantes :
1.3.1. Réparer/reconstruire au moment de l'incident.
1.3.2. Déplacer la production vers une autre ligne.
1.3.3. Déplacer la production vers un autre site similaire.
1.3.4. Réoutiller la production sur le site concerné.
1.3.5. Utiliser l'inventaire existant.
1.3.6. Utiliser la capacité excédentaire d'autres usines.
1.3.7. Suspendre, interrompre ou réduire la production.
1.3.8. Racheter le produit aux clients et le redistribuer.
1.3.9. Proposer un produit de substitution à la place des produits non disponibles.
1.3.10. Externaliser la production.

2. Protéger les documents papier essentiels qui risquent d'être détruits.
2.1. Les documents doivent être numérisés régulièrement vers un stockage en nuage ou une autre solution de stockage hors site afin de répondre aux objectifs de rétablissement des documents essentiels. Si une entité choisit d'utiliser des photocopies de documents, celles-ci doivent être stockées dans un lieu hors site. Notez que les exigences légales relatives aux documents non originaux peuvent varier d'une juridiction à l'autre. Vérifiez la validité de l'utilisation de copies ou d'images numériques à la place des documents originaux.
2.2. Évaluer les options de sites alternatifs en utilisant les critères suivants selon le cas :
2.2.1. Emplacement
2.2.2. Accessibilité
2.2.3. Disponibilité et la pertinence de l'espace
2.2.4. Capacité de communication incluant la voix et les données
2.2.5. Disponibilité du matériel et des fournitures
2.2.6. Exigences en matière de robustesse et la durabilité du site, y compris la disponibilité de ressources telles que l'électricité et l'eau
2.3. Évaluer la viabilité des stratégies alternatives avec les exigences énoncées dans le bilan des impacts d'affaires en utilisant les critères suivants :
2.3.1. Capacité à atteindre les objectifs de rétablissement définis
2.3.2. Comparaison des solutions potentielles, y compris les avantages et les inconvénients, et analyse de coûts/bénéfices
2.4. Réviser les couvertures existantes en assurances.
2.4.1. Les types d'assurance peuvent inclure, sans s'y limiter, les éléments suivants :
2.4.1.1. Cyber
2.4.1.2. Dépenses supplémentaires
2.4.1.3. Interruption d'activités
2.4.1.4. Interruption d'activités collatérales
2.4.1.5. Responsabilité civile
2.4.1.6. Salaire
2.4.1.7. Biens et risques divers
2.4.1.8. Catastrophes naturelles (assurance contre les inondations)
2.4.2. Intégrer une couverture d'assurance qui peut être utilisée pour soutenir le processus de rétablissement.
2.4.3. Effectuer une analyse de coûts/bénéfices. Comparer les résultats attendus des stratégies potentielles aux impacts définis dans l'évaluation des risques et le bilan des impacts d'affaires.

3. Utiliser les données recueillies au cours de l'évaluation des risques et du bilan des impacts d'affaires pour identifier les stratégies de continuité et de reprise de la technologie de l'entité afin d'atteindre les objectifs de temps de rétablissement et objectifs de point de rétablissement définis dans le bilan des impacts d'affaires.
    3.1. Réviser les exigences de rétablissement identifiées pour la technologie de l'entité dans chaque domaine opérationnel.
    3.2. Identifier des stratégies alternatives de reprise technologique. Les options potentielles incluent, mais ne sont pas limitées à :
        3.2.1. Élaborer des solutions alternatives manuelles pour chaque domaine opérationnel.
        3.2.2. Mettre en place une solution technologique répondant aux objectifs de reprise.
        3.2.3. Envisagez plusieurs centres de données pour disperser les données et les opérations au niveau régional.
        3.2.4. Utiliser des systèmes à haute disponibilité permettant un redémarrage rapide.
        3.2.5. Utiliser des services tiers.
        3.2.6. Tirez parti de l'informatique en nuage.
    3.3. Identifier un site de reprise avec des contrôles environnementaux adéquats.
    3.4. Identifier l'équipement technologique pour soutenir une main-d'œuvre distante.
    3.5. Développer une analyse de coûts/bénéfices des stratégies retenues pour les solutions technologiques de l'entité.
    3.6. Identifier tout problème logistique, réglementaire ou financier qui pourrait survenir.
    3.7. Identifiez les stratégies potentielles de la chaîne d'approvisionnement pour minimiser les impacts basés sur l'évaluation des risques et du bilan des impacts d'affaires.
    3.8. Collaborer avec des représentants de l'industrie, des agences gouvernementales et d'autres contacts externes pour échanger des informations afin de déterminer des stratégies potentielles.
4. Identifier les problèmes de la chaîne d'approvisionnement (pour les fournisseurs et les clients) à partir du bilan des impacts d'affaires qui peuvent affecter la sélection de la stratégie de rétablissement.
    4.1. Identifier les problèmes de livraison qui pourraient résulter de la relocalisation sur un autre site.
5. Évaluer les coûts de mise en œuvre des stratégies identifiées grâce à une analyse coûts/bénéfices.
    5.1. Évaluer les coûts de mise en place et de maintenance des stratégies de rétablissement identifiées.
    5.2. S'assurer que les stratégies mises en œuvre sont en fonctions des domaines opérationnels impactés.
        5.2.1. Tenir compte des facteurs financiers et réglementaires.
        5.2.2. S'assurer que les stratégies respectent les objectifs de rétablissement.
        5.2.3. S'assurer que le coût de rétablissement est conforme à la valeur de ce qui doit être rétabli.
    5.3. Tenez compte de la réduction de l'impact financier que la couverture d'assurance fournit pour déterminer les stratégies qui bénéficient d'une assurance telle que l'interruption d'activités, interruption d'activités collatérales, la chaîne d'approvisionnement, la cyber et l'assurance sur les dépenses supplémentaires.
6. Recommander des stratégies et obtenir l'approbation de la direction pour leur mise en œuvre.
    6.1. Documenter les recommandations pour approbation par la direction.
    6.2. Obtenir l'approbation de la direction.

Pratique professionnelle 5: Préparation et interventions d'urgence

Objectifs

1. Comprendre les types d'incidents qui pourraient menacer la vie, les biens, les opérations ou l'environnement et leurs impacts potentiels.
2. Établir et maintenir des capacités pour protéger la vie, les biens, les opérations et l'environnement contre les incidents potentiels grâce à la mise en œuvre d'un système de gestion des incidents pour commander, contrôler et coordonner les activités d'intervention, de continuité et de rétablissement avec des ressources internes et externes.

Rôle du professionnel

1. Identifier les dangers qui pourraient menacer la vie, endommager des biens, interrompre les opérations ou contaminer l'environnement.
2. Identifier les réglementations applicables en matière de santé et de sécurité, d'incendie, de sécurité des personnes, de sécurité nationale, d'environnement, de cybersécurité et de sécurité de l'information applicables par les autorités fédérales, provinciales, régionales et/ou locales.
3. Identifier la disponibilité et les capacités des ressources internes et externes nécessaires pour protéger la vie, les biens et l'environnement pour les types d'incidents identifiés.
4. Identifier et évaluer les plans de préparation et de réponse aux incidents en fonction de l'évaluation des risques et des vulnérabilités des actifs à risque, ainsi que de la disponibilité et des capacités des ressources internes et externes existantes.
5. Effectuer une évaluation des besoins en ressources.
6. Réviser les plans de préparation et de réponse aux incidents.
7. Recommander l'élaboration et aider à la mise en œuvre d'un système de gestion des incidents pour le commandement, le contrôle et la coordination des ressources pendant les activités d'intervention.
8. Réviser les plans et procédures de préparation et d'intervention en cas d'incident avec le personnel d'intervention, et aider à la coordination des agences et ressources internes et externes pertinentes.
9. Obtenir et documenter l'approbation officielle des plans et des procédures par la direction.

Activités

1. Identifier les dangers qui pourraient menacer la vie, endommager des biens, interrompre les opérations ou contaminer l'environnement.
   - 1.1. Les catégories d'aléas comprennent les aléas naturels (biologiques, géologiques, météorologiques), les actes accidentels et intentionnels d'origine humaine (chimiques, nucléaires) et les causes liées à la technologie.
   - 1.2. Pour chaque catégorie de danger, identifiez les scénarios prévisibles et notez les informations suivantes :
     - 1.2.1. Probabilité d'occurrence
     - 1.2.2. Ampleur ou portée
     - 1.2.3. Zone(s) d'impact
     - 1.2.4. Vulnérabilités des actifs à risque qui les rendent sensibles au danger
     - 1.2.5. Stratégies de prévention et d'atténuation existantes
   - 1.3. Pour chaque type d'incident, identifiez les impacts potentiels, y compris, mais sans s'y limiter, les victimes, les dommages matériels, la contamination de l'environnement, la réputation, les finances, la réglementation et/ou l'incapacité à mener des activités essentielles à la mission.
2. Identifier les réglementations applicables en matière de santé et de sécurité, d'incendie, de sécurité des personnes, de sécurité nationale, d'environnement, de cybersécurité et de sécurité de l'information applicables par les autorités fédérales, provinciales, régionales et/ou locales.
   - 2.1. Se conformer aux exigences réglementaires et aux exigences des entités en matière de préparation et de réponse aux incidents.

3. Identifier la disponibilité et les capacités des ressources internes et externes nécessaires pour protéger la vie, les biens et l'environnement pour les types d'incidents identifiés.
    3.1. Identifier et établir des relations avec les départements internes et les agences externes qui ont des responsabilités en matière de préparation et de réponse aux incidents.
    3.2. Recueillir des plans de préparation et d'intervention en cas d'incident auprès des ressources internes, y compris la santé, la sécurité et l'environnement, la sécurité, la gestion des installations, les ressources humaines et autres.
    3.3. Contacter les organismes publics, y compris, mais sans s'y limiter, la sécurité publique, la gestion des urgences, les services médicaux d'urgence, les services d'incendie, les forces de l'ordre, les matières dangereuses, le sauvetage et la réponse aux cyberincidents, afin d'identifier les exigences, les pratiques et les ressources, et d'établir des relations de liaison.
4. Identifier et évaluer les plans de préparation et de réponse aux incidents en fonction de l'évaluation des risques et des vulnérabilités des actifs à risque, ainsi que de la disponibilité et des capacités des ressources internes et externes existantes.
    4.1. Mesures de sécurité des personnes, y compris, mais sans s'y limiter, l'évacuation, la mise à l'abri, le confinement, "courir, se cacher, se battre", et la responsabilité du personnel intervenant ou affecté par l'incident.
    4.2. Protocoles de santé, d'hygiène et de sécurité, y compris la réponse aux urgences médicales.
    4.3. Protection de la propriété telle que la supervision et l'exploitation des systèmes et équipements du bâtiment, y compris les services publics ; chauffage, ventilation et climatisation (CVC); détection et extinction des incendies ; et les systèmes de communication et d'alerte.
    4.4. Activités de conservation des biens pour préparer une installation en prévision de conditions météorologiques extrêmes ou à un autre incident perturbateur.
    4.5. Endiguement des déversements ou des fuites de matières dangereuses pour prévenir les blessures et la contamination de l'environnement. Supervision et exploitation de systèmes conçus pour contenir des matières dangereuses sur le site. Exigences relatives à la notification et au signalement des incidents aux autorités environnementales.
    4.6. Temps de réponse et capacités du service public d'incendie, des services médicaux d'urgence, du service de secours et de l'entrepreneur en matières dangereuses.
5. Effectuer une évaluation des besoins en ressources.
    5.1. Ressources nécessaires pour protéger la vie, les biens et l'environnement.
    5.2. Personnel interne et externe qualifié pour répondre aux incidents.
    5.3. Systèmes et équipements, y compris, mais sans s'y limiter, les systèmes de détection, d'alarme, de communication, d'avertissement, d'extinction et de confinement, disponibles pour la réponse aux incidents.
    5.4. Les accords d'aide mutuelle ou de partenariat applicables sont documentés et à jour.
    5.5. Écarts entre les ressources requises et la disponibilité et la capacité des ressources internes et externes.
    5.6. Écarts entre les exigences et la disponibilité et les capacités des ressources.
6. Réviser les plans de préparation et de réponse aux incidents.
    6.1. Surveiller les menaces et les aléas et détecter rapidement les incidents.
    6.2. Avertir les personnes en danger ou potentiellement en danger de prendre des mesures de protection.
    6.3. Alerter les premiers intervenants internes et externes.
    6.4. Signaler les incidents à la personne, au service et/ou à l'agence responsable.
    6.5. Escalader la réponse en fonction de l'analyse de la situation.
7. Recommander l'élaboration et aider à la mise en œuvre d'un système de gestion des incidents pour le commandement, le contrôle et la coordination des ressources pendant les activités d'intervention.
    7.1. Développer une organisation de gestion des incidents avec des rôles définis, des responsabilités, des lignes d'autorité, des délégations d'autorité et une succession d'autorité.

7.2. Acquérir une compréhension des systèmes de commandement et de gestion des incidents au niveau local, provincial et fédéral.
7.3. Élaborer des procédures pour l'analyse de la situation, l'élaboration d'un plan d'action en cas d'incident, la gestion des ressources internes et externes et l'approvisionnement en ressources supplémentaires.
7.4. Développer des procédures pour les breffages sur les incidents, y compris les rapports de situation initiaux et périodiques.
7.5. Documenter les communications lors d'un incident.
7.6. Établir un centre des opérations d'urgence (COU) physique ou virtuel pour la coordination des activités d'intervention, de continuité et de rétablissement.
7.6.1. Les centres d'opérations d'urgence physiques doivent être dimensionnés pour accueillir le nombre de personnes prévu et équipés pour soutenir la gestion des incidents identifiés pendant la durée.
7.6.2. Le centre des opérations d'urgence doit être équipé des types de capacités de communication nécessaires pour prendre en charge l'étendue et la durée des incidents prévisibles.
7.6.3. Des procédures doivent être établies pour la gestion du centre d'opérations d'urgence, les opérations, la planification, la logistique et les finances/administration, définissant les rôles et les responsabilités, les communications et le flux d'informations. Des copies sécurisées des politiques, plans et procédures doivent être immédiatement disponibles pour le personnel du centre d'opérations d'urgence.

8. Réviser les plans et procédures de préparation et d'intervention en cas d'incident avec le personnel d'intervention, et aider à la coordination des agences et ressources internes et externes pertinentes.
8.1. Identifier les documents, tels que les plans préincidents, les plans d'action d'urgence et les plans de gestion des matières dangereuses, qui doivent être soumis aux organismes publics.
9. Obtenir et documenter l'approbation officielle des plans et des procédures par la direction.

Pratique professionnelle 6: Élaboration et mise en œuvre du plan

Objectifs

1. Documenter les plans à être utilisé lors d'un incident qui permettra à l'entité de continuer à fonctionner.
2. Définir les critères d'exercice / test pour vérifier que les plans permettront d'atteindre l'objectif souhaité.

Rôle du professionnel

1. Utiliser les stratégies approuvées élaborées dans la Pratique professionnelle 4 : Stratégies de continuité des activités comme base pour la documentation du plan.
2. Définir la structure de la documentation du plan.
3. Coordonner les efforts de documentation des plans de rétablissement des activités de l'entité et des technologies qui les soutiennent. Considérez les types de plans en fonction des besoins de l'entité.
4. Publier les plans documentés.

Activités

1. Utiliser les stratégies approuvées élaborées dans la Pratique professionnelle 4 : Stratégies de continuité des activités comme base pour la documentation du plan.
    1.1. Concevoir, élaborer et mettre en œuvre des stratégies de rétablissement pour les opérations de l'entité.
        1.1.1. Identifier les besoins qui seront utilisés dans la création du plan de continuité des activités.
        1.1.2. Rendre compte de l'avancement de l'élaboration et de la mise en œuvre du plan aux autorités désignées.[1]
        1.1.3. Accomplir toutes les tâches requises pour la mise en œuvre du plan, ce qui peut inclure, mais sans s'y limiter :
            1.1.3.1. Acquérir des ressources internes et externes en matière de plans de reprise et de continuité des activités
            1.1.3.2. Établir des processus d'intervention, de rétablissement et de restauration
            1.1.3.3. Établir des processus pour le développement et la maintenance de la documentation
2. Définir la structure de la documentation du plan.
    2.1. Déterminer comment le plan sera organisé et identifier les équipes nécessaires pour documenter les plans.
        2.1.1. Assurer l'alignement avec la portée du processus de planification.
        2.1.2. Des plans complets de continuité des activités traitent des ressources, des personnes, des installations et de la technologie. Les composants du plan de continuité des activités peuvent inclure des exigences réglementaires, stratégiques (délégation d'autorité), opérationnelles, interventions d'urgence, de rétablissement, de restauration et de retour aux opérations normales.
        2.1.3. Les considérations stratégiques peuvent inclure, mais ne sont pas limitées à :
            2.1.3.1. Le délai de préalerte
            2.1.3.2. Si la durée est courte ou longue
            2.1.3.3. Si les impacts sont locaux ou régionaux, ou spécifiques aux sites d'une entité
            2.1.3.4. S'il existe un potentiel d'impact en cascade provoqué par un événement en cascade. Un événement en cascade se produit lorsque l'incident a le potentiel de créer des effets négatifs supplémentaires.
    2.2. Définir les rôles et les responsabilités pour le développement du plan, y compris les actions suivantes :
        2.2.1. Identifier les tâches à accomplir, y compris les exercices/tests.
        2.2.2. Élaborer un échéancier pour compléter le Plan, y compris les exercices/tests.

[1] Voir Pratique professionnelle 1 : Gestion du programme pour plus de détails sur la définition de la structure hiérarchique.

2.2.3. Développer un processus de révision, d'évaluation et de recommandation d'outils, qui peut inclure, mais sans s'y limiter, un logiciel de planification, un logiciel d'exercice/de test, des bases de données, un logiciel spécialisé et des gabarits.
2.2.4. Élaborer des gabarits qui peuvent être utilisés pour capturer des informations sur les processus, la technologie et d'autres composants du plan.
2.2.5. Identifier tout autre besoin de soutien à la documentation.
2.2.6. S'assurer que des mécanismes soient intégrés pour faciliter la maintenance, tels qu'un contrôle de version défini.

2.3. Définir les exigences de contenu pour le plan, pouvant inclure, mais sans se limiter à :
2.3.1. Gouvernance, politiques et procédures, contrôle de la distribution, exigences de confidentialité et niveaux d'autorité.
2.3.2. La portée et les objectifs, y compris les hypothèses, alignés sur la mission, les buts, les objectifs et les politiques de continuité des activités de l'entité, y compris l'identification des opérations sensibles au facteur temps et les ressources nécessaires pour les soutenir.
2.3.3. Les structures organisationnelles des équipes ainsi que les rôles et responsabilités de chaque équipe.
2.3.4. Procédures d'activation du plan : évaluation initiale, escalade, processus de notification, déclaration, activation du plan, rétablissement, annulation de la déclaration et reprise des opérations normales.

3. Coordonner les efforts de documentation des plans de rétablissement des activités de l'entité et des technologies qui les soutiennent. Considérez les types de plans en fonction des besoins de l'entité.

3.1. Plan(s) de gestion des incidents, qui doivent inclure les éléments suivants :
3.1.1. Procédures de sécurité des personnes, y compris l'évacuation et la mise à l'abri.
3.1.2. Procédures de commandement et de contrôle de l'incident.
3.1.3. Rôles et responsabilités du personnel participant à la gestion de l'incident.
3.1.4. Emplacement du centre des opérations d'urgence (COU).
3.1.5. Le processus de réalisation d'une évaluation, qui devrait comprendre :
3.1.5.1. Limiter l'entité à d'autres pertes, y compris une analyse coûts/avantages de la réparation par rapport au remplacement des actifs de l'entité.
3.1.5.2. Délai estimé nécessaire pour réparer ou remplacer les ressources de l'entité.
3.1.5.3. Méthodes de restauration des ressources de l'entité.
3.1.5.4. Processus d'autorisation pour la restauration et la déclaration de sinistre.
3.1.5.5. Processus de sauvetage.

3.2. Plan(s) de gestion de crise [2], qui devraient inclure les éléments suivants :
3.2.1. Membres de l'équipe de gestion de crise.
3.2.2. Un aperçu des procédures d'interventions d'urgence, de communication de crise et de rétablissement.
3.2.3. Procédures de notification aux parties prenantes à intervalles appropriés pendant un incident (telles que les mises à jour sur la situation, des communiqués de presse et d'autres communications ciblées conçues pour les parties prenantes), qui peuvent inclure, mais sans s'y limiter, les médias, les employés et leurs familles, les organismes réglementaires, les premiers répondants, les agences, services spécialisés pour les matières dangereuses (HAZMAT), les investisseurs, le conseil d'administration ou toute autre autorité compétente, les représentants syndicaux, les occupants voisins et d'autres groupes intéressés (tels que les clients, les vendeurs ou les fournisseurs).

3.3. Plan(s) d'activation du site de rétablissement, qui doivent inclure les éléments suivants :
3.3.1. Procédures d'alerte.
3.3.2. Procédures de déclaration.
3.3.3. L'infrastructure de rétablissement, pouvant inclure:
3.3.3.1. Administration et logistique.
3.3.3.2. Nouveaux équipements ou livraisons juste-à-temps.
3.3.3.3. Les services et procédures techniques.
3.3.3.4. Relation avec les utilisateurs.

[2] Voir aussi Pratique professionnelle 5 : Préparation et interventions d'urgences et Pratique professionnelle 9 : Communication de crise.

3.3.3.5. Activités d’affaires.
3.3.3.6. Logistique et communication intersites.
3.3.3.7. Processus et procédure de rétablissement de la production.
3.3.3.8. Logistique impliquée dans l'organisation du déplacement et de l'hébergement du personnel de rétablissement ; transporter les ressources nécessaires à la reprise, à l'entretien et à la sécurité du site de reprise ; et soumettre l'acquisition de ressources supplémentaires.

3.4. Plan(s) de reprise opérationnelle, y compris :
3.4.1. Les équipes de rétablissement, y compris les membres principaux et les substituts.
3.4.2. Les ressources requises pour la documentation incluant, mais sans le limiter aux requis technologiques, dossiers essentiels, communication voix et données, contacts ou fournisseurs clés et équipements requis.

3.5. Plan(s) de continuité des activités, qui doivent inclure les éléments suivants :
3.5.1. Équipes de rétablissement, y compris les membres principaux et substituts.
3.5.2. Moyens alternatifs de mener les activités lorsque les ressources normales ne sont pas disponibles.
3.5.3. Processus, procédures et communication en matière de continuité des activités.
3.5.4. Mobilisation de ressources alternatives.
3.5.5. Gestion des ressources alternatives.

3.6. Plan(s) de reprise technologique, qui doivent inclure les éléments suivants :
3.6.1. Équipes de reprise comprenant des membres principaux et substituts.
3.6.2. Mobiliser et gérer des ressources alternatives, y compris les ressources qui peuvent être nécessaires pour :
3.6.2.1. Stockage, qui peut inclure, mais sans s'y limiter, les périphériques de stockage en réseau et les périphériques de stockage de données.
3.6.2.2. Matériel de communication voix et données, qui peut inclure, mais sans s'y limiter, des commutateurs de réseau local (LAN), des commutateurs d'alimentation sur Ethernet et des commutateurs gérés/non gérés.
3.6.2.3. Exigences matérielles et logicielles, qui peuvent inclure, mais sans s'y limiter, les serveurs, les lecteurs de bande/bibliothèque de bandes, les logiciels d’application, les systèmes d'exploitation, les applications et les logiciels de sécurité.
3.6.2.4. Les exigences d'infrastructure, qui peuvent inclure, mais sans s'y limiter, les sources d'alimentation et les contrôleurs ; chauffage, ventilation et climatisation (CVC); câblage ; et accès sécurisés.
3.6.2.5. Exigences en matière de sécurité des informations, qui peuvent inclure, mais sans s'y limiter, les pare-feu, l'authentification d'accès, la protection contre les logiciels malveillants, le cryptage et les exigences en matière d'équipement.
3.6.3. Le(s) plan(s) de reprise de la technologie doivent(vent) décrire une procédure détaillée pour la reprise des environnements technologiques, y compris les étapes suivantes :
3.6.3.1. Identifier l'application et les dépendances.
3.6.3.2. Un processus de gestion des changements.
3.6.3.3. Un processus de gestion des problèmes.
3.6.3.4. Un plan pour les exercices/tests et la maintenance.

3.7. Plan(s) pour annuler le(s) plan(s) d'activation du site de rétablissement et autres mesures d'urgence.

4. Publier les plans documentés.
4.1. Fournir une version finale du plan, y compris les recommandations d'exercices/de tests, aux propriétaires des processus d'affaires.
4.2. Obtenir l'approbation de la direction.
4.3. Établir des procédures pour la distribution et le contrôle des plans.
4.4. S'assurer que l'accès aux informations est disponible même lorsque l'environnement informatique est compromis.
4.5. Publier et distribuer les plans ou des parties des plans à ceux qui sont autorisés à recevoir des informations.

Pratique professionnelle 7: Programmes de sensibilisation et de formation

Objectifs

1. Établir et maintenir des programmes de formation et de sensibilisation qui permettent au personnel de répondre aux incidents perturbateurs de manière calme et efficace.

Rôle du professionnel

1. Définir les objectifs et composantes du programme de sensibilisation et formation en continuité des activités.
2. Identifier les besoins en matière de sensibilisation et de formation dans toutes les fonctions de l'entité.
3. Prioriser les besoins en matière de sensibilisation et de formation pour le personnel de l'entité.
4. Élaborer la méthodologie du programme de sensibilisation et de formation pour l'entité.
5. Identifier, acquérir ou développer les outils et les ressources de sensibilisation et de formation nécessaires pour atteindre les objectifs du programme.
6. Superviser la prestation des activités menées pour atteindre les objectifs du programme de sensibilisation et de formation.

Activités

1. Définir les objectifs et composantes du programme de sensibilisation et formation en continuité des activités.
   - 1.1. Définir le programme de sensibilisation et de formation.
   - 1.2. Recommander un calendrier de sensibilisation et de formation.
   - 1.3. Obtenir le soutien de la direction pour le programme.
   - 1.4. Obtenir l'engagement du personnel.
2. Identifier les besoins en matière de sensibilisation et de formation dans toutes les fonctions de l'entité.
   - 2.1. Définir et documenter le niveau souhaité de sensibilisation et de formation à la continuité des activités dans l'ensemble de l'entité.
   - 2.2. Définir et documenter les besoins en ressources et en budget pour la sensibilisation et la formation.
3. Prioriser les besoins en matière de sensibilisation et de formation pour le personnel de l'entité.
   - 3.1. Lors de la conception d'un programme de sensibilisation, il est important de déterminer quel personnel interne doit comprendre les composants pertinents du programme de continuité des activités. Les sujets incluent, mais ne sont pas limités à :
     - 3.1.1. Objectifs, portée et composants du programme de continuité des activités
     - 3.1.2. Notification et attentes en cas d'incident, ainsi que des procédures de préparation et d'intervention en cas d'incident.
   - 3.2. Lors de la conception d'un programme de formation, il est important de déterminer quel personnel doit être formé dans quels composants du programme de continuité des activités. Les sujets obligatoires dans lesquels le personnel doit être formé peuvent inclure, mais sans s'y limiter :
     - 3.2.1. Rapport d'incident.
     - 3.2.2. Notifications d'alerte.
     - 3.2.3. Procédures d'évacuation et de mise à l'abri.
     - 3.2.4. Des exercices basés sur des scénarios qui permettent de tester les opérations et les éléments du plan de continuité des activités technologiques.
   - 3.3. La formation requise en matière de gestion peut comprendre, sans s'y limiter, les éléments suivants :
     - 3.3.1. Exercices/tests d'identification et de réaction aux incidents.
     - 3.3.2. Revue détaillée basée sur un scénario d'opérations et de technologies.
   - 3.4. Les sujets obligatoires sur lesquels les membres de l'équipe de continuité des activités doivent être formés peuvent inclure, mais sans s'y limiter:
     - 3.4.1. Exercices/tests d'évacuation et d'abri sur place.
     - 3.4.2. Revue détaillée basée sur un scénario.

3.4.3. Exercices technologiques.

4. Élaborer la méthodologie du programme de sensibilisation et de formation pour l'entité.
   4.1. Réaliser une évaluation des besoins du programme de sensibilisation et de formation pouvant inclure, mais sans se limiter aux méthodes suivantes :
      4.1.1. Mener un sondage sur les besoins pour évaluer l'état actuel de la sensibilisation et de la formation afin de déterminer s'il est conforme aux objectifs fixés par la direction. Les participants au sondage peuvent être à différents niveaux et peuvent inclure diverses parties telles que les gestionnaires des unités fonctionnelles, les participants au plan, la technologie et toutes autres personnes de l'organisation.
      4.1.2. Utiliser les données collectées pour identifier les tendances et les écarts.
      4.1.3. Revoir les résultats des exercices/tests précédents et effectuer des analyses d'écarts.
   4.2. Comparer les niveaux actuels de sensibilisation et de formation au sein de l'entité par rapport aux niveaux souhaités et lancer un plan pour combler les écarts en matière de sensibilisation et de formation.
   4.3. Concevoir le processus de formation pour inclure les éléments suivants :
      4.3.1. Définir les objectifs, identifier et sélectionner les méthodes de livraison, y compris, mais sans s'y limiter, les exercices/tests basés sur des scénarios et les communications.
      4.3.2. Définir les rôles et les responsabilités pour le programme de formation.
      4.3.3. Créer un plan de formation écrit et des politiques de soutien.
      4.3.4. Obtenir l'approbation de la direction.
5. Identifier, acquérir ou développer les outils et les ressources de sensibilisation et de formation nécessaires pour atteindre les objectifs du programme.
   5.1. Identifier les ressources internes et externes nécessaires pour soutenir le programme de sensibilisation et de formation, qui peuvent inclure, mais sans s'y limiter, des didacticiels, des sites Web, des outils de médias sociaux, des applications, des conférences, des webinaires, des groupes et associations d'utilisateurs et des associations, des mémoires et d'autres publications, des organismes pertinents de certification et programmes d'enseignement universitaire.
6. Superviser la prestation des activités menées pour atteindre les objectifs du programme de sensibilisation et de formation.
   6.1. Planifier et mener des activités de sensibilisation.
   6.2. Planifier et animer des activités de formation.
   6.3. Mesurer l'efficacité des activités de sensibilisation et de formation à l'aide de sondages ou d'auto-évaluation par les participants.
   6.4. Examinez périodiquement les résultats des activités du programme de sensibilisation et de formation. Fournir un rapport à la direction sur les résultats du programme.
   6.5. Évaluer périodiquement le programme de sensibilisation et de formation pour s'assurer que les besoins actuels de l'entité sont satisfaits.
   6.6. S'assurer que le programme de sensibilisation fait partie du processus d'accueil des nouveaux employés.

Pratique professionnelle 8: Exercice/test, évaluation et maintenance du plan de continuité des activités

Objectifs

1. Établir un plan d'exercice/test de continuité des activités, d'évaluation, et de programme de maintenance afin d'améliorer l'état de préparation de l'entité.

Rôle du professionnel

1. Définir un programme de test et d'exercice.
2. Définir un programme de maintenance.
3. Identifier une gouvernance appropriée.
4. Définir un processus d'audit du programme de la continuité des activités.
5. Fournir des recommandations écrites basées sur les résultats de l'exercice/du test, y compris des révisions des stratégies et des plans si les résultats souhaités ne peuvent pas être atteints.

Activités

1. Définir un programme de test et d'exercice.
    - 1.1. Développer un programme d'exercices et de tests répondant à la portée et les objectifs du programme de continuité des activités de l'entité.
        - 1.1.1. S'assurer que le programme de continuité des activités documenté répond à ses objectifs.
        - 1.1.2. Identifier toute lacune dans le programme de continuité des activités et fournir des solutions pour éliminer les lacunes et améliorer l'exécution du programme.
    - 1.2. Obtenir le soutien et les approbations de leadership nécessaires pour le développement du programme d'exercices/tests.
        - 1.2.1. Documenter les critères du programme d'exercices/tests.
        - 1.2.2. Définir les hypothèses du programme d'exercices et de tests.
        - 1.2.3. Afin de créer un programme complet, identifiez les types d'exercices/tests qui seront inclus dans le programme d'exercices/tests. Ceux-ci peuvent inclure, mais sans s'y limiter, les éléments suivants : la sécurité des personnes ; d'une revue de plan ; exercice de table basé sur des scénarios ; notification; site alternatif; infrastructure ou application ; processus fonctionnel; exercice complet du début à la fin d'une activité ou d'une technologie ; exercice/test complet de toutes les ressources internes nécessaires pour redresser l'entité ; et exercice/test entièrement intégré couvrant les dépendances internes et externes.
        - 1.2.4. Identifier les participants et leurs rôles et responsabilités dans le programme d'exercices/tests, qui peuvent inclure, mais sans s'y limiter, les équipes de rétablissements, les observateurs/scribes, les contrôleurs, les auditeurs/réviseurs, les animateurs, les fournisseurs et les prestataires de services externes.
        - 1.2.5. Utilisez les priorités d'atténuation de l'évaluation des risques de l'entité (consultez la Pratique professionnelle 2 : Évaluation des risques) pour créer des scénarios réalistes. Inclure les activités qui font référence aux stratégies de rétablissement et à la capacité d'atteindre les objectifs dans les délais établis. Déterminer les exigences des exercices/tests et rédiger un plan détaillé des activités.
            - 1.2.5.1. Définir et documenter les objectifs de l'exercice/du test.
            - 1.2.5.2. Définir et documenter la portée de l'exercice/du test.
            - 1.2.5.3. Définir le processus de notification de l'exercice, qui peut inclure des exercices annoncés ou non annoncés. Élaborer un calendrier précis pour l'exercice/test qui sera réalisé au moins une fois par an ou plus fréquemment pour répondre aux exigences réglementaires ou aux changements dans la structure de l'entité (ce qui peut inclure des acquisitions et des fusions, des réorganisations, des consolidations, des ventes de parties de l'entité) et/ou les opérations. Élaborer un calendrier d'exercices/tests pluriannuel qui tient compte des leçons tirées des exercices/tests précédents et qui contient de plus en plus d'éléments d'entité aux exercices/tests.

1.2.5.4. Définir et documenter les critères d'évaluation quantitatifs et qualitatifs en fonction des objectifs de l'exercice/test. Il s'agit notamment de mesurer les résultats de l'exercice/test par rapport aux objectifs de temps de rétablissement et aux objectifs de point de rétablissement définis dans le bilan des impacts d'affaires. Déterminer les activités qui doivent avoir lieu avant l'exercice/test, qui peuvent comprendre, sans s'y limiter, les éléments suivants :
1.2.5.4.1. Identifiez les ressources nécessaires pour effectuer l'exercice/le test.
1.2.5.4.2. Identifier les participants nécessaires pour participer à l'exercice/test.
1.2.5.4.3. Distribuez des communications qui expliquent les objectifs de l'exercice/du test et les rôles de toutes les parties (y compris les forces de l'ordre, les services d'urgence et les médias). Fournir une liste du matériel, des logiciels, des fournitures, de l'équipement et d'autres ressources nécessaires pour l'exercice/test.
1.2.5.4.4. Documenter et communiquer les besoins en ressources nécessaires pour effectuer l'exercice/le test.
1.2.5.4.5. Indiquez si l'exercice ou test utilisera un environnement de production ou de non-production.
1.2.5.4.6. Précisez l'heure, la date et le(s) lieu(x) de l'exercice/du test. Fournir un calendrier des événements et le faire circuler à tous les participants.
1.2.5.4.7. Établir un plan d'annulation de l'exercice/test au cas où l'exercice/test ne parviendrait pas à atteindre les objectifs spécifiés, ce qui exclut la possibilité que l'exercice/test se termine comme prévu.

1.2.6. Mener l'exercice ou le test tel que planifié.
1.2.6.1. Si un événement survient durant l'exercice, vous devriez avoir un mécanisme préétabli pour annuler l'exercice et activer le processus de continuité des activités en place. Cela diffère du plan d'annulation de 1.2.5.4.7.
1.2.6.2. Enregistrer les événements de l'exercice/test.
1.2.6.3. Documenter les résultats de l'exercice/test.
1.2.6.4. Déclarer la fin de l'exercice/test.
1.2.6.5. Effectuez les procédures d'arrêt à la conclusion de l'exercice/test.
1.2.6.6. Effectuez toutes les activités de nettoyage nécessaires.

1.2.7. Identifier les activités post-exercice qui doivent être accomplies.
1.2.7.1. Organiser des séances de débreffage pour réviser les résultats de l'exercice/test. Identifier les leçons apprises et les mesures d'amélioration.
1.2.7.2. Rapport sur les résultats de l'exercice/test. Fournir un résumé complet des recommandations.
1.2.7.3. Documenter un plan d'action pour les recommandations qui ont résulté de l'exercice/test.
1.2.7.4. Noter tous les problèmes en suspens identifiés à la suite de l'exercice/test ou qui existaient avant l'exercice/test.
1.2.7.5. Identifier les éléments d'action, y compris les responsabilités attribuées à des participants spécifiques et les échéanciers.
1.2.7.6. Surveiller la progression jusqu'à l'achèvement des éléments d'action identifiés. Documenter les leçons tirées de l'exercice/test, y compris les résultats attendus par rapport aux résultats réels et les résultats inattendus.
1.2.7.7. Communiquer les résultats de l'exercice/test.

2. Définir un programme de maintenance.
2.1. Définir la méthodologie et le calendrier de maintenance.
2.1.1. Définissez la propriété des éléments du plan. Identifier le personnel spécifique et leurs domaines de responsabilité.
2.1.2. Préparer le calendrier de maintenance et les procédures de révision.
2.1.3. Créer des procédures pour faciliter la maintenance du plan.
2.1.4. Choisir les outils de maintenance.
2.1.5. Assurer le suivi des activités de maintenance.
2.1.6. Établir un processus de contrôle des changements pour le plan.

2.2. S’assurer que la maintenance planifiée du plan répond à toutes les recommandations approuvées de l'exercice/test. Rendre compte des activités de maintenance aux parties prenantes. Définir un processus de gestion du changement pour le programme de maintenance du plan.
    2.2.1. Analyser tout changement d'entité qui entraînerait des mises à jour du programme de continuité des activités et du processus de planification. Élaborer des procédures de contrôle des changements pour surveiller les changements. Intégrer ces procédures à tout processus de contrôle des changements existant.
    2.2.2. Établir un contrôle des versions adéquat. Élaborer des procédures pour la réédition, la distribution et la diffusion du plan aux parties prenantes.
    2.2.3. Identifier les listes de distribution du plan.
    2.2.4. Élaborer un processus pour mettre à jour les plans en fonction de la réponse aux constatations de l'audit.
    2.2.5. Mettre en œuvre le processus de contrôle des changements.
3. Identifier une gouvernance appropriée.
    3.1. Examiner les attentes des parties organisationnelles, qui peuvent inclure les réglementations, les directives de santé publique, les exigences de l'industrie, les besoins internes de l'entité, les accords de niveau de service, et/ou d'autres facteurs environnementaux. Identifier les processus à l'échelle de l'entité, y compris un processus récurrent de révision, d'amélioration et de perfectionnement continue.
    3.2. Identifier les modèles de gouvernance appropriés en fonction de l'industrie, ou des normes nationales et internationales.
    3.3. Définir la fréquence et la portée des exercices ou de tests qui répond aux besoins de l'entité.
    3.4. Assurer l'approbation par les parties organisationnelles désignées.
4. Définir un processus d’audit[3] du programme de la continuité des activités.
    4.1. Déterminer un calendrier pour effectuer un audit de première partie (auto-évaluation).
    4.2. Se préparer à soutenir d'autres audits qui peuvent se produire, qui peuvent inclure, mais ne sont pas limités à, l'audit interne ou l'audit externe tel que la seconde partie (client), la tierce partie, ou l'organisme de réglementation / gouvernement. Documenter toute exigence d'audit.
    4.3. Sélectionner ou développer les outils qui peuvent être nécessaires pour effectuer l'audit.
    4.4. Mener des activités d'audit et surveiller le processus. L’audit de la structure du Plan, du contenu et des sections d'action du plan peut inclure, mais sans s'y limiter, les exigences, les documents et les normes du programme ; gabarits et plans; exigences en matière d’exercices/tests et leurs résultats; planifier l'entretien ; la consignation du plan et les résultats des exercices/tests ; les procédures de contrôle de la documentation du plan ; le processus et la documentation de contrôle des versions; et les listes de distribution et processus associés.
    4.5. Effectuer l’Audit du processus de contrôle des changements pour la documentation du plan et le programme de la continuité des activités.
    4.6. Réviser les réponses aux constatations de l’Audit.
    4.7. Vérifier que les actions complétées ont été consignées au plan et dans la documentation de soutien.
5. Fournir des recommandations écrites basées sur les résultats de l'exercice/du test, y compris des révisions des stratégies et des plans si les résultats souhaités ne peuvent pas être atteints.
    5.1. Obtenir l'approbation de la direction pour apporter des révisions aux stratégies et aux plans au besoin. Identifier les parties organisationnelles pertinentes, qui peuvent inclure, mais sans s'y limiter, les propriétaires de processus, les coordonnateurs de la gouvernance, les comités de surveillance et la direction de l'organisation.
    5.2. Sélectionnez les méthodes de communication, y compris le niveau de détail des rapports. Envisagez des représentations graphiques ou des rapports de comparaison destinés à des auditoires spécifiques en coordination avec l'équipe de communication de l'entité. Établir un processus de surveillance garantissant que les mesures appropriées ont été prises à la suite des constatations d'audit signalées. Ce processus doit inclure le suivi des problèmes, le responsable de la correction du problème, la date cible pour l'achèvement de la correction et les dates d'ouverture/fermeture de l’élément.

[3] Aux fins du présent document, le terme audit désigne à la fois les audits et les évaluations.

Pratique professionnelle 9: Communication de crise

Objectifs

1. Créer et maintenir un plan de communication de crise.
2. Veiller à ce que le plan de communication de crise permette une communication rapide et efficace avec les parties internes et externes.

Rôle du professionnel

1. Concevoir, élaborer et mettre en œuvre un plan de communication de crise.
2. Communiquer et former les membres de l'équipe de communication de crise sur leurs rôles et responsabilités.
3. Exercer le plan de communication de crise.
4. Examiner et mettre à jour le plan de communication de crise au moins une fois par an ou plus fréquemment si les résultats des exercices/tests, les réglementations ou les modifications apportées à l'entité le justifient.

Activités

1. Concevoir, élaborer et mettre en œuvre un plan de communication de crise.
    - 1.1. Revoir tout plan de communication de crise existant, en identifiant et en documentant les écarts.
    - 1.2. Exploitez les résultats de l'évaluation des risques comme indiqué dans la pratique professionnelle n° 2 : Évaluation des risques afin d'identifier les incidents potentiels pour lesquels des communications doivent être planifiées.
    - 1.3. Définir les objectifs, la portée et la structure du plan.
    - 1.4. Établir l'emplacement, les rôles et les responsabilités de l'équipe de communication de crise.
        - 1.4.1. Identifier et documenter l'emplacement principal des opérations de l'équipe de communication de crise. Il peut s'agir d'un emplacement physique ou virtuel. Identifier un site secondaire.
        - 1.4.2. Identifier la structure de gouvernance pour le développement de la communication interne.
        - 1.4.3. Identifier la fonction qui servira de contact principal pour les communications externes avec les médias.
    - 1.5. Identifier les parties prenantes internes et externes pour les communications de crise. Ils peuvent inclure, mais sans s'y limiter, la recherche des contacts de santé publique, les employés et leurs familles, les investisseurs, les clients, les vendeurs et les fournisseurs, les opérations imparties, les organisations de partage d'informations sur la cybersécurité, les assureurs, les dirigeants communautaires, les autorités locales d'intervention, les organismes gouvernementaux, les législateurs, les organisations syndicales, les concurrents, les médias, les blogueurs de l'industrie et publications spécialisées, et autres parties prenantes ou impliquées.
    - 1.6. Développer et documenter le processus de notification des parties prenantes.
        - 1.6.1. Déterminer le ton, le contenu et la fréquence des communications avant, pendant et après l'incident.
        - 1.6.2. Identifier les moyens de communication, qui peuvent inclure, mais sans s'y limiter, les réunions présentielles, les appels téléphoniques personnels, les visites à domicile, les systèmes de notification d'incident, des listes de courriels et de groupe de distribution, les appels-conférences, les systèmes intranet, les conférences de presse, des lignes d'information sur l'incident, sources médiatiques (telles que la presse écrite, la radio, la télévision), Internet, les plateformes de médias sociaux et les blogues/vlogues.
    - 1.7. Établir des lignes directrices pour identifier un événement et ses impacts potentiels.
    - 1.8. Établissez des lignes directrices pour la communication initiale avant, pendant et après un incident.
    - 1.9. Identifier et affecter des membres à l'équipe de communication de crise.
    - 1.10. Obtenir l'approbation de la direction du plan de communication de crise et du processus de notification.
    - 1.11. Élaborer des lignes directrices pour les communications avec l'équipe d'intervention d'urgence.
    - 1.12. Documentez des exemples de communications pouvant être utilisés comme modèles lors d'un incident.

1.13. S'assurer qu'il existe un processus d'approbation pour toutes les communications sortantes.

2. Communiquer et former les membres de l'équipe de communication de crise sur leurs rôles et responsabilités.
   2.1. Distribuer le plan de communication de crise à ceux qui se sont vu attribuer des rôles et des responsabilités.
   2.2. Offrir une formation à ceux qui se sont vu attribuer des rôles et des responsabilités. La formation peut inclure, mais sans s'y limiter, les éléments déclencheurs pour démarrer le processus de communication de crise, les procédures de notification, d'approbation et de réponse, ainsi que les outils appropriés pour émettre des communications.
3. Exercer le plan de communication de crise.
   3.1. Établir un calendrier d'exercices/tests pour le plan de communication de crise qui est conforme à la Pratique professionnelle 8 : Exercice/test, évaluation et maintenance du plan de continuité des activités. S’assurer que le plan de communication de crise soit intégré à tous les exercices/tests.
   3.2. Déterminer la méthodologie pour exercer/tester le plan de communication de crise.
   3.3. Élaborer le scénario, la portée et les objectifs de chaque exercice ou test.
   3.4. Effectuez un débreffage pour déterminer les leçons apprises après l'exercice/test. Documenter les éléments d'action corrective.
4. Examiner et mettre à jour le plan de communication de crise au moins une fois par an ou plus fréquemment si les résultats des exercices/tests, les réglementations ou les modifications apportées à l'entité le justifient.

Pratique professionnelle 10: Coordination avec les agences et ressources externes

Objectifs

1. Établir des politiques et des procédures pour coordonner les activités d'intervention avec les entités publiques et les ressources privées applicables, conformément à la pratique professionnelle cinq : Préparation et interventions d'urgence.

Rôle du professionnel

1. Identifier et établir des procédures d'intervention d'urgence pour l'entité conformément à la pratique professionnelle 5 : Préparation et intervention d'urgence.
2. Identifier les directives applicables en matière de préparation et d'intervention d'urgence et les organismes ayant juridiction sur l'entité.
3. Coordonner les procédures d'intervention d'urgence avec les agences et ressources externes.

Activités

1. Identifier et établir des procédures d'intervention d'urgence pour l'entité conformément à la pratique professionnelle 5 : Préparation et intervention d'urgence.
2. Identifier les directives applicables en matière de préparation et d'intervention d'urgence et les organismes ayant juridiction sur l'entité.
   - 2.1. Identifier les organismes de réglementation ayant compétence sur l'entité. Les agences peuvent inclure, mais sans s'y limiter, la santé publique, les responsables des installations, les pompiers, les forces de l'ordre, les organismes de réglementation, la sécurité et la santé au travail et d'autres organisations gouvernementales.
   - 2.2. Identifier les exigences pour la soumission d'informations sur les installations de l'entité (telles qu'une description des espaces occupés, des dangers, des systèmes de protection et des et d'intervention d'urgence) aux organisations appropriées, y compris celles identifiées à la section 2.1.
   - 2.3. Identifier les exigences en matière d'inspection périodique d'édifice, incluant la fréquence de formation et d'exercices/tests.
   - 2.4. Identifier les exigences et les délais pour la déclaration obligatoire des incidents.
   - 2.5. Élaborer ou mettre à jour les procédures de préparation et d'intervention d'urgence pour se conformer aux lois, règlements et autres directives autorisées par le gouvernement. Coordonner avec les équipes de conformité et/ou juridiques de l'entité.
   - 2.6. Distribuer les informations prescrites aux organismes de réglementation.
   - 2.7. Surveiller les modifications apportées aux lois, règlements et directives. Modifier les procédures pour maintenir la conformité.
   - 2.8. Obtenir l'approbation de la direction des procédures d'intervention d'urgence avec des agences externes.
3. Coordonner les procédures d'intervention d'urgence avec les agences et ressources externes.
   - 3.1. Identifier l'agence et/ou la ou les ressources qui agiront en tant que premiers répondants lors de l'incident.
   - 3.2. Développer et documenter les procédures et les exigences d'alerte d'urgence (telles que le signalement obligatoire des matières dangereuses, des blessures et d'autres incidents).
   - 3.3. Identifier les représentants des agences/ressources des premiers répondants et établir des relations de liaison avec le personnel concerné.
   - 3.4. Inviter le personnel des agences/ressources de premiers répondants à visiter les installations de l'entité et leur demander de fournir des recommandations pour améliorer les plans d'intervention d'urgence.
   - 3.5. Identifier et documenter les rôles et les responsabilités en matière de réponse aux interventions d'urgences pour les types d'urgences et les scénarios de gestion de la continuité des activités, comme indiqué dans la pratique professionnelle 5 : Préparation et interventions d'urgence.
   - 3.6. Coordonner, mener et participer à des exercices/tests avec des agences/ressources et des premiers répondants pour accroître la sensibilisation et la conformité aux réglementations.

3.7. Tenir une session de rétroaction après les exercices/activités de test. Documenter les résultats des exercices/tests, les leçons apprises et les actions à entreprendre pour améliorer les capacités d'intervention.
3.8. Fournir les résultats des exercices/tests à la direction et aux autres fonctions organisationnelles désignées.
3.9. Mettre à jour les plans d'intervention d'urgence en utilisant les leçons apprises et les commentaires des exercices/tests conformément au calendrier établi dans la pratique professionnelle 8 : Exercice/test, évaluation et maintenance du plan de continuité des activités.