Business
Continuity Plan

Document : Historique

**HISTORIQUE DES VERSIONS DU DOCUMENT**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Dates | Modifié par | Articles modifiés (V +1) |
| xxx | xxx | xxx | xxx |
| … |  |  |  |

**HISTORIQUE DES VALIDATIONS**

|  |  |  |
| --- | --- | --- |
| Nom | Fonction | Date de la validation par le plus haut niveau de direction |
| xxx | xxx | xxx |
| … |  |  |

Le présent document s’applique à compter du **[date].**

Ce document est conservé comme suit:

1. Sur papier, aux endroits suivants: **[Indiquer les lieux]**.
2. Sous forme numérique aux endroits suivants: **[localisation sur l’intranet, par exemple]**.

Le titulaire de ce document est **[fonction]**. Il vérifie au moins 1 fois par an si des mises à jour sont nécessaires.

**Table des Matières**

[**Chapitre I Objectif du document** 4](#_Toc57020880)

[**Chapitre II Liens entre les procédures** 5](#_Toc57020881)

[**Chapitre III Placez un pilote dans l’avion** 7](#_Toc57020882)

 [3.1 Désignez un gestionnaire pour le plan de continuité des activités 7](#_Toc57020883)

 [3.2. Rôles du Gestionnaire du plan de continuité des activités 7](#_Toc57020884)

[**CHAPITRE IV PLAN DE CONTINUITE DES ACTIVITES** 9](#_Toc57020885)

 [4.1 Etape 1 : Délimitation du champ d’application du plan de continuité des activités 9](#_Toc57020886)

 [4.2 Etape 2 : Activation du plan 10](#_Toc57020887)

 [4.3 Etape 3 : Etablissez la liste des actions à entreprendre 13](#_Toc57020888)

 [4.4 Etape 4 : Désactivation du plan de continuité des activités 17](#_Toc57020889)

 [4.5 Etape 5 : Testez votre plan et maintenez-le à jour 18](#_Toc57020890)

[**Chapitre V Annexes** 19](#_Toc57020891)

 [5.1. Annexe 1 : Liste des contacts 19](#_Toc57020892)

 [A) Internes 19](#_Toc57020893)

 [B) Externes 21](#_Toc57020894)

 [5.2. Annexe 2: Documents de référence 21](#_Toc57020895)

# Chapitre IObjectif du document

**Le principal objectif** d’un Business Continuity Plan (BCP) est **d’assurer la continuité des (principales) activités de l’entreprise** même en cas d’incident, de crise ou de désastre.

**Comment ?** Il s’agit de :

1. **Anticiper** et adopter une approche cohérente pour la réalisation d’un Business Continuity Plan afin d’identifier les processus les plus importants et d’analyser les risques auxquels ils sont exposés ;
2. **Élaborer des procédures** adaptées pour savoir comment réagir face à un incident, à une crise ou à un désastre
3. I**dentifier les éléments nécessaires** (matériel, bâtiment, personnes en interne et en externe,....) pour mettre en œuvre efficacement les procédures validées par le plus haut niveau de direction de l’entreprise afin de gérer les incidents, crises et désastres.

**Résultat ?**

1. **Disposer de procédures validées**
2. **Savoir comment diminuer l’impact** de ces incidents à un niveau acceptable pour l’entreprise.
3. **Obtenir des objectifs et une définition des temps impartis** pour assurer la continuité des (principales) activités de l’entreprise.

ATTENTION : même si les procédures ont été validées, ***n’oubliez pas d’assurer un reporting régulier auprès de la direction*** en cas d’incident ayant un impact sur la continuité des activités de l’entreprise.

**Menaces** : La gestion de la continuité est plus large que les éventuels incidents informatiques. Des inondations ou des incendies, l’absence de collaborateurs (maladie, licenciement, décès), la disparition d’un ou de plusieurs fournisseur.s essentiel.s à l’entreprise, des pandémies,...peuvent également constituer une menace pour la continuité des activités de l’entreprise. Lors de l’organisation de la gestion de la continuité, et plus particulièrement dans le risk assessment, il s’agit d’identifier tous les types de menaces qui peuvent peser sur les activités de l’entreprise en ayant également à l’esprit le “worst case scenario”.

*Concernant l’identification des menaces, des vulnérabilités et de l’impact : Voir votre Risk Assessment et votre Risk Treatment.*

# Chapitre II Liens entre les procédures

Le schéma (voir ci-dessous) indique comment le Business Continuity Plan s’intègre avec les autres procédures.

1. Pour disposer d’un plan de continuité des activités efficace, cela suppose que vous avez rempli les templates Risk Assessment et Risk Treatment. Le niveau de risques et la probabilité d’un incident dépendent du Risk Treatment que vous aurez effectué. De même, la gestion d’un incident dépendra beaucoup des mesures préventives et curatives que vous aurez mises en place.
2. En construisant votre Business Continuity Plan et votre plan de gestion des incidents, il est possible que vous deviez remettre à jour votre Risk Assessment (notamment par ce que vous envisagez de modifier les risques en acquérant de nouveaux outils ou en lançant de nouveaux projets).
3. Votre Risk Assessment et votre plan de continuité des activités présupposent également que vous vous renseigniez auprès de vos fournisseurs, que vous examiniez vos contrats voire que vous imposiez certains niveaux de service (Service Level Agreement SLA) ou certaines clauses auprès de vos fournisseurs.
4. La continuité des activités de l’entreprise a des liens étroits avec la gestion des incidents car vous devez vous assurer que même lors d’un incident vous pourrez continuer les activités (au moins essentielles) de l’entreprise. Le gestionnaire du plan de continuité des activités de l’entreprise transmet les informations nécessaires au gestionnaire du plan de gestion des incidents.
5. Vous pourriez notamment prendre connaissance d’un incident en cours par le biais de vos clients ou de vos fournisseurs.
6. La plupart des incidents n’impliquent pas forcément l’activation du plan de continuité des activités de l’entreprise simplement parce qu’il s’agit de petits incidents “habituels” qui n’ont pas d’impact réel sur les activités. Si un incident ayant un impact sur les activités survient, le gestionnaire des incidents avertit le gestionnaire du plan de continuité des activités qui active le plan de continuité des activités. Pendant l’incident, par le gestionnaire des incidents assure un reporting régulier auprès du gestionnaire du plan de continuité. Après l’incident, le gestionnaire des incidents transmet le “Post incident review” au gestionnaire du plan de continuité.
7. Si l’incident n’a pas d’impact sur la continuité des activités, le gestionnaire du plan de gestion des incidents peut avertir, si besoin, les clients et fournisseurs que l’entreprise rencontre un incident mineur.
8. Si l’incident a un impact sur la continuité des activités, le gestionnaire du plan de continuité des activités s’adresse, si besoin, aux clients et fournisseurs en fonction des éléments d’information qui lui sont transmis par les services fonctionnels ainsi que par le gestionnaire du plan de gestion des incidents.
9. Après un incident, le post incident review vous indiquera peut être qu’il faudrait modifier le risk assessment et le risk treatment
10. Après un incident, le post incident review vous indiquera peut être qu’il faudrait réviser les contrats auprès de vos fournisseurs

Après une gestion des incidents, il est possible que vous deviez revoir votre risk assessment et votre risk treatment ou que votre plan de continuité des activités de l’entreprise doive être amélioré. **Pour plus d’informations concernant les différentes procédures, consultez les templates mis à votre disposition.**

Pour que le plan élaboré fonctionne efficacement en cas d'incident, il est important que les **procédures** prévues soient **testées de manière approfondie au préalable et révisées régulièrement**. Au moins une fois par an et après chaque incident/crise ou catastrophe, pensez à réviser vos plans et à déterminer les "leçons apprises" afin de pouvoir améliorer les plans en fonction des besoins et de l'expérience de l'entreprise.

Toutes les personnes impliquées dans le plan de continuité des activités de l’entreprise doivent connaître leur rôle exact et disposer de la version la plus récente de ce plan. (Pensez à en conserver une version papier également).

**1. Risk Assessment & Risk Treatment**

**2. Business Continuity Plan**

**3. Gestion des
incidents**

**Fournisseurs
essentiels**

**Clients**

**B**

**A**

**B**

**C**

**D**

**E**

**E**

**F**

**H**

**G**

**G**

**I**

**H**

**J**

**A**

# Chapitre IIIPlacez un pilote dans l’avion

## 3.1 Désignez un gestionnaire pour le plan de continuité des activités

*“Everything that* can *go wrong* will *go wrong”*

*Murphy’s Law*

L’incident vous tombera peut être dessus un vendredi soir, un week end, la veille d’un gros contrat ou d’une période de fêtes,...

Mieux vaut penser aux incidents avant que se retrouver complètement démuni face à un incident...

N’oubliez pas de placer “un pilote dans l’avion” et de désigner une autre personne qui pourrait le remplacer en cas d’absence/départ/maladie.

*Qui choisir ?* Idéalement, ce “pilote” doit être un bon communicateur, connaître suffisamment bien l’entreprise, être résilient au stress et disposer de suffisamment d’expérience.Dans les plus grandes structures, *u*ne “team” peut être désignée.

Il peut s’agir de la direction ou d’une personne qui dispose de l’autorité requise pour assurer un rôle opérationnel stratégique.

Attention, gestionnaire ne veut pas toujours dire “responsable”, le gestionnaire peut devoir s’appuyer sur plusieurs responsables internes mais il est évident que les décisions majeures et la responsabilité finale relève du plus haut niveau de direction. C’est pourquoi il importe que toutes les procédures soient validées par la direction.

## 3.2. Rôles du gestionnaire du plan de continuité des activités

Le gestionnaire du plan de continuité des activités doit s’assurer de maintenir un dialogue constructif au sein de l’entreprise, favoriser la collaboration entre les services ou personnes impliquées et assurer le reporting auprès de la direction.

Le gestionnaire du plan de continuité des activités (qu’il s’agisse d’une personne ou du leader d’une équipe en fonction de la taille et des besoins de l’entreprise) :

1. Rassemble la Business Continuity Team (s’il y en a une) et prend contact avec la ou les personnes ressources clefs (services IT, conseiller en sécurité et prévention, délégué à la protection des données, conseiller en sécurité de l’information....) ;
2. Tient une première réunion (avec la Business Continuity Team si elle existe et à défaut avec la direction) afin d’évaluer l’impact de l’incident et de déterminer le niveau de criticité de l’incident ainsi que les activités impactées. (Il est possible de ré-évaluer la situation en fonction des circonstances. Il ne s’agit ici que d’une première évaluation) ;
3. Avertit la direction et assure un reporting régulier auprès d’elle ;
4. Active le plan de continuité des activités ;
5. Identifie si possible comment l’incident pourrait évoluer. Déterminez quelles informations manquent encore afin de mieux comprendre la situation et comment ces informations seront recueillies dans un délai précis. (Attention, il ne s'agit pas de recueillir *toutes* les infos à ce stade mais uniquement les plus urgentes c’est à dire celles qui sont nécessaires à une première évaluation du niveau de criticité actuel et probable de l’incident) ;
6. Prend contact, si besoin, avec le service de communication et le service de relations à la clientèle (s’ils existent) ou propose à la direction un plan de communication vers les clients et fournisseurs si besoin (voir gestion des incidents, Fiche “Communication”) ;
7. Prend contact avec les responsables fonctionnels concernés et leur transmet les informations recueillies à ce stade ;
8. Maintient le dialogue avec les services fonctionnels concernés, et assure le reporting au niveau de la direction tout au long de l’incident ;
9. Peut ordonner la dégradation ou l’interruption d’une activité non essentielle en vue de disposer des ressources nécessaires pour les activités essentielles ;
10. Peut organiser l’évacuation des employés et clients ;
11. Peut communiquer avec les clients et fournisseurs (communication externe) ;
12. Met fin à l’activation du plan de continuité des activités de l’entreprise ;
13. Participe au post incident review une fois que l’incident a pris fin ;
14. Assure la révision des plans (modifications éventuelles en fonction des besoins et de l’expérience acquise) et la validation des plans par la direction ;
15. Organise les exercices et tests nécessaires pour sensibiliser et mettre à jour le plan de continuité des activités
16. Tient les plans à disposition des personnes clefs (y compris sous format papier et hors zone inondable) ;
17. *…[Identifiez les autres rôles éventuels.]*

NB : Dans certaines structures, il est possible :

* qu’une seule et même personne ou équipe assume la gestion de tous les incidents.
* que des externes soient associés aux démarches. Par exemple, un cabinet d’avocats, des délégués à la protection des données externes, des assureurs,....
* que certaines étapes n’aient pas lieu (comme les étapes 6 et 7 par exemple).

# CHAPITRE IVPLAN DE CONTINUITE DES ACTIVITES

*“In preparing for battle, I have always found that plans are useless, but planning is indispensable.”*

*General Dwight D. Eisenhower*

Il est impossible de tout prévoir, des évènements soudains et imprévisibles peuvent toujours survenir.

Lorsqu’un incident survient, votre plan n’aura peut-être pas “pensé à tout” mais le simple fait que vous vous soyez préparé pour d’autres types d’incident et que vous ayez entamé une réflexion sur la continuité de vos activités vous permettra de mieux résister et de pouvoir continuer à assurer les activités au moins essentielles de votre entreprise.

Un plan de continuité de l’entreprise (business continuity plan) repose sur 5 étapes :

Étape 1: Délimitation du champ d’application du plan de continuité des activités

Étape 2 : Activation du plan

Étape 3 : Désactivation du plan

Étape 4 : Testez et maintenez votre plan à jour

## 4.1 Etape 1 : Délimitation du champ d’application du plan de continuité des activités

Un plan de continuité des activités de l’entreprise est un processus itératif.

Pour une première itération, concentrez-vous sur l’essentiel : Quelles activités sont essentielles pour la survie économique de votre entreprise ? Vous pourriez notamment tenir compte :

* de la part des revenus que ces activités génèrent ;
* du nombre de clients qui les demandent ;
* de l’impact si l’activité devait subir une dégradation ou une interruption : impact sur la productivité, sur les finances et/ou sur la réputation de l’entreprise.

Vous pourriez limiter votre plan de continuité des activités à ces activités essentielles dans un premier temps.

NB : Votre Risk Assessment devrait déjà vous avoir aidé à y voir plus clair à ce stade.

| Activité essentielle 1 |
| --- |
| Liste des éléments essentiels pour assurer la continuité de l’activité essentielle concernée  |
| Personnel clef |
| Information ou données clefs |
| Service informatique (hardware, software) nécessaire |
| Bâtiments |
| ... |

## 4.2 Etape 2 : Activation du plan

Le gestionnaire du plan de continuité des activités peut notamment activer le plan parce que les autorités ou le régulateur sectoriel ont pris des mesures d’ordre, parce des fournisseurs ont indiqué une pénurie d’un élément essentiel, ou parce que le gestionnaire du plan de gestion des incidents l’a averti qu’il pourrait y avoir un impact sur la continuité des activités de l’entreprise...

|  |
| --- |
| **SAFETY FIRST : Protégez La vie humaine d’abord !** |

Cela va sans dire bien sûr mais avant même de s’assurer de la continuité des activités de l’entreprise, il s’agit de protéger la vie humaine d’abord. Ceci implique également de prendre les mesures appropriées en fonction des circonstances de l’entreprise.

Un focus particulier devrait être accordé aux risques d’incendie, d’explosion, d’exposition à des produits toxiques, d’inondation,...

Le gestionnaire ou l’équipe en charge du plan de continuité des activités procède aux vérifications et/ou actions suivantes pour assurer le bien-être des personnes :

1. Identification des scenarios d’incident
2. Identification des types de risques
3. Mesures de prévention
4. Mesures de gestion
5. Post incident review.

Ce schéma est identique au plan de gestion des incidents que le gestionnaire du plan de continuité prendra soin de connaître.

**Exemple**

**Scenario :** des produits dangereux s’écoulent ou s’évaporent anormalement, des personnes armées s’introduisent dans les bâtiments, une épidémie ou une pandémie sévit dans la région où se situent les lieux de travail ou à proximité, l’eau potable est contaminée, un incendie ou une inondation menace les lieux habituels de travail (incendie en cours dans un bâtiment proche, proximité de zones déjà inondées et zone inondable),...

**Risques** : Mise en danger du personnel, blessures, morts et séquelles psychologiques à envisager.

**Mesures de prévention :**

* Identifier le cadre Juridique obligatoire (Code du bien-être au travail,...) et consulter le site web du [SPF Emploi](https://emploi.belgique.be/fr/themes/bien-etre-au-travail), celui de l’[European Agency for Safety and Health at work](https://oiraproject.eu/en/oira-tools) et le Centre de connaissance belge sur le bien-être au travail ([BeSWIC](https://www.beswic.be/fr))
* Se conformer aux obligations légales et/ou réglementaires (détecteurs d’incendie, portes coupe-feu,...).
* Identifier les personnes ressources indispensables et définir les rôles et responsabilités avant tout incident
* Identifier les numéros de secours et les moyens de les contacter
* Prévoir un défibrillateur dans le bâtiment
* Sensibiliser le personnel aux bonnes pratiques (ne pas fumer dans les locaux, ne pas laisser des portes ou fenêtres ouvertes, signaler immédiatement tout incident pouvant mettre en danger autrui, former son personnel aux notions de base de secourisme,...)
* Prévoir des plans d’évacuation (incendie, inondation,...) et les tester régulièrement (au moins une fois par an).
* Identifier les personnes plus à risques (ayant des difficultés pour se déplacer, pour respirer,...ou qui sont particulièrement sensibles (difficultés cardiaques, respiratoires,...

**Mesures de gestion d’incident**

En fonction du niveau de criticité de l’incident, l’incident est une première fois qualifié par le gestionnaire du plan de gestion d’incident. S’il y a un risque d’impact sur les activités de l’entreprise, le gestionnaire du plan de gestion des incidents avertit le gestionnaire du Business Continuity Plan. (NB : dans les plus petites structures, il est possible qu’une seule et même personne assume ces différentes fonctions).

Cette première évaluation est rapide et peut devoir être revue en cours d’incident.

|  | Action | Qui fait quoi ? | Liens vers d’autres documents |
| --- | --- | --- | --- |
|  | Description de l’action | Fonctions et rôles des personnes clefs charges d’accomplir l’action | Référence des autres documents |
|[ ]  Prendre connaissance des obligations légales en matière de prévention des risques professionnels, de sécurité et de protection de la santé au travail. |  |  |
|[ ]  Consulter le site web du BESWIC : <https://www.beswic.be/fr> Des check list sont disponibles auprès du SPF Emploi en fonction du type d’évènement redouté (pandémie,...)Des outils sont également mis à disposition par l’European Agency for Safety and Health at Work<https://oiraproject.eu/en/oira-tools>  |  |  |
|[ ]  Disposer des procédures adéquates (gestion des incidents) |  |  |
|[ ]  Définir les rôles et responsabilités (avant tout incident)  |  |  |
|[ ]  Identifier toutes les mesures de gestion (voir gestion des incidents) |  |  |
|[ ]  Identifier et tenir à jour la liste des services d’urgence et personnes internes et externes ressources |  |  |
|[ ]  Informer le personnel et si besoin les parties prenantes externes (clients, fournisseurs) qu’un incident est cours et que des mesures sont prises pour le traiter. |  |  |
|[ ]  Conserver les journaux d’incidents (logs, preuves, traces) |  |  |
|[ ]  Penser à prendre régulièrement contact avec les (familles des) blesses éventuels |  |  |
|[ ]  … |  |  |

## 4.3 Etape 3 : Etablissez la liste des actions à entreprendre

N’oubliez pas votre Risk Assessment et votre Risk Treatment : vous avez déjà pris de nombreuses mesures pour réduire le risque ou limiter l’impact d’un incident. Si vous envisagez d’autres actions en établissant votre plan de continuité des activités, n’oubliez pas de maintenir à jour votre Risk Assessment et votre Risk Treatment. Le plan de continuité des activités est également lié au plan de gestion des incidents (voir template Gestion des incidents).

Le gestionnaire ou l’équipe de continuité des activités prend les mesures nécessaires pour atténuer et minimiser les dommages causés par l’incident et pour maintenir les activités essentielles. Lorsque vous rédigez votre plan de continuité des activités, vous pouvez notamment dresser des listes de contrôle (check list). Notez toutefois qu’il est impossible d’identifier tous les scenarios d’incident et qu’il est beaucoup plus important que l'équipe soit capable de s’adapter aux circonstances. Une fois le personnel concerné sensibilisé à ces plans, l’entreprise sera plus à même de mieux réagir quel que soit l’incident rencontré.

*Remplissez ce tableau en tenant compte de la situation de votre entreprise :*

| **Actions** | **Qui fait quoi ?** | **Liens vers d’autres documents**  |  |
| --- | --- | --- | --- |
| Description de l’action | Fonctions et rôles des personnes clefs charges d’accomplir l’action | Référence des autres documents | Ok ? |
| Identifier les processus et activités importants qui sont perturbés et décrire l'impact sur la prestation de services. |  |  |  |
| Identifier le (risque de) préjudice, tant matériel qu'immatériel (par exemple la réputation) |  |  |  |
| Identifier les actions visant à garantir que la situation ne s'aggrave pas davantage * Faites valider ces choix par la Direction
 |  |  |  |
| Identifier ce qui est intact ("ce qui fonctionne encore") |  |  |  |
| Actions visant à déployer des ressources supplémentaires, tant par le biais de son propre personnel que par celui des sous-traitants.* Faites valider ces choix par la Direction
 |  |  |  |
| … |  |  |  |

#### Scenario: le bâtiment principal n’est pas accessible

| Élément(Description) | Dommages (Description) | Actions et instructions | Temps de récupération estimé |
| --- | --- | --- | --- |
| Ex : grève nationale bloquant l’accès de votre site principal,Ex coupure de courant ou délestage d’électricité rendant l’accès impossible ou malaisé | Identifier les processus et activités importants qui sont perturbés et décrire l'impact sur la prestation de services.Identifier le (risque de) préju-dice, tant matériel qu'immatériel (par exemple la réputation)Identifier ce qui est intact ("ce qui fonctionne encore") | Etablir la liste des mesures préventives *(liens avec le Risk Treatment et le plan de gestion des incidents)*Etablir la liste des mesures de gestion *Identifier les actions visant à garantir que la situation ne s'aggrave pas davantage**Identifier les actions visant à déployer des ressources supplémentaires, tant par le biais de son propre personnel que par celui des sous-traitants.*Ex : mettre les travailleurs en télétravail (pour ceux qui ne font pas grève), avertir les fournisseurs de ne pas livrer à l’adresse habituelle, avertir les clients de ne pas se rendre au bâtiment principal et préciser l’impact éventuel sur les délais de livraison, Ex : contacter l’électricien ou le gestionnaire de réseau de distribution d’électricité (voir également les mesures précitées). | Ex : 1 jour, 1 semaineEx : 4 heures ou 1 semaine,... |
| … |  |  |  |

#### Scenario : interruption de la connexion au cloud ou au data center

| Élément(Description) | Dommages(Description) | Actions et instructions | Temps de récupération estimé |
| --- | --- | --- | --- |
| Votre entreprise n'a plus accès aux données et fichiers qui n'ont pas été sauvegardés localement. | Identifier quelles sont les activités essentielles (voir étape 1) qui seront impactées et déterminer l’impact pour ces activités. | Établir la liste des mesures préventives *(liens avec le Risk Treatment et le plan de gestion des incidents)* Ex : Conserver au moins une copie locale,...Établir la liste des mesures de gestion *Identifier les actions visant à garantir que la situation ne s'aggrave pas davantage**Identifier les actions visant à déployer des ressources supplémentaires, tant par le biais de son propre personnel que par celui des sous-traitants.* Ex : contacter le fournisseur de services cloud ou le responsable du data center et déterminer le temps de récupération estimé, demander à être tenu au courant en temps réelEx : appliquer les sanctions contractuelles pour non-respect du niveau de service convenu (SLA). | Par ex : 5h ou 2 jours |

#### Scenario: inondation

| Élément(Description) | Dommages (Description) | Actions et instructions | Temps de récupération estimé |
| --- | --- | --- | --- |
| Une inondation  | Identifier quelles sont les activités essentielles (voir étape 1) qui seront impactées et déterminer l’impact pour ces activités. | Établir la liste des mesures préventives *(liens avec le Risk Treatment et le plan de gestion des incidents)* VOIR FICHE INONDATIONÉtablir la liste des mesures de gestion *Identifier les actions visant à garantir que la situation ne s'aggrave pas davantage**Identifier les actions visant à déployer des ressources supplémentaires, tant par le biais de son propre personnel que par celui des sous-traitants*Ex : télétravail pour les employés, contacter les assureurs, procéder à l’évacuation manuelle ou pneumatique des eaux boueuses,... | Par ex : une semaine |

#### Scenario: …

| Élément(Description) | Dommages (Description) | Actions et instructions | Temps de récupération estimé |
| --- | --- | --- | --- |
| .....  |  | ... | .... |

## 4.4 Etape 4 : Désactivation du plan de continuité des activités

La désactivation du plan de continuité des activités est réalisée par le gestionnaire du plan de continuité des activités, en accord avec la direction.

Le plan de continuité des activités peut notamment être désactivé quand l’incident est clos ou qu’il n’y a pas/plus d’impact sur les activités essentielles de l’entreprise (même si l’incident est encore en cours, par exemple parce qu’une solution temporaire a pu être trouvée).

|  **Critères de désactivation du plan de continuité des activités** |
| --- |
| Tous les niveaux de service sont-ils revenus à la normale ou au niveau minimum acceptable ? |
| Y a-t-il des raisons de douter que les niveaux de service seront atteints de manière stable dans les prochains jours?  |
| Les mesures de gestion (y compris les solutions temporaires) ont-elles été désactivées?  |
| Les équipes opérationnelles (services fonctionnels) sont-elles suffisamment équipées pour faire face aux conséquences potentielles postérieures à l’incident?  |
| La communication finale vers les externes (clients, fournisseurs,...) a t elle eu lieu ?  |
| ... |

Dans le cadre de la désactivation du plan de continuité, il y a lieu de décrire les évènements pour pouvoir améliorer la prochaine activation du plan.

| **Actions** | **Qui fait quoi ?** | **Liens vers d’autres documents** |
| --- | --- | --- |
| Description brève des actions (mesures de gestion) qui ont été prises |  |  |
| Faire référence au post incident review |  |  |
| Contacter les assureurs |  |  |
| Dresser une communication “fin de crise” à l’attention des personnes externes concernées (clients, fournisseurs) |  |  |
| Établir si des points du plan de continuité pourraient être améliorés (y compris dans le cadre des relations contractuelles externes) |  |  |
| Application des éventuelles sanctions contractuelles lorsque les niveaux de services (SLA) n’ont pas été respectés. |  |  |

**Le Post incident Review**

Il s’agit de joindre Post incident review au rapport de désactivation du plan de continuité des activités. (Voir Plan de Gestion des incidents et les fiches).

## 4.5 Etape 5 : Testez votre plan et maintenez-le à jour

***“Un plan qui dort sur une étagère ne vaut pas le papier sur lequel il est imprimé”***

En effet, si le plan de continuité des activités prend la poussière, il y a de fortes chances qu’en cas d’incident personne ne sache comment l’appliquer. Une sensibilisation régulière est nécessaire.

Pensez à entraîner le personnel et envisagez divers canaux de communication (posters, fléchage, exercices, outils). Pour des idées d’outils voir : [BeSWIC](https://www.beswic.be/fr/en-pratique/loutil-dinstruction-toworksafe-pour-la-securite-des-travailleurs-allophones) concernant la sécurité des travailleurs ; [Cyber Security Coalition](https://www.cybersecuritycoalition.be/fr/resource/cyber-security-kit/) concernant la cybersécurité; [SPF Emploi](https://emploi.belgique.be/fr/actualites/coronavirus-materiel-de-sensibilisation-sur-le-lieu-de-travail-en-17-langues) concernant les pandémies;...

|  |  |  |
| --- | --- | --- |
| **Mesures** | **Commentaires** | **Ok ?** |
| Désigner un gestionnaire **et** une personne en cas d’absence du gestionnaireouDésigner une équipe en charge pour le plan de continuité des activités (et un leader) |  |  |
| Fournir une formation au personnel au moins une fois par an et lorsque des mises à jour importantes sont élaborées |  |  |
| Effectuer un exercice régulièrement (au moins une fois par an) |  |  |
| S’assurer de disposer des contacts nécessaires (fournisseurs, avocats, assureurs,...) et vérifier que les contacts sont bien à jour (au moins une fois par an) |  |  |
| Tester les procédures de sauvegarde et de récupération des données au moins régulièrement (idéalement trimestriellement) |  |  |
| Actualiser le plan de continuité en fonction des personnes (arrivée/départ) et des circonstances (nouveaux projets, nouvelles gestion des procédures internes,...) |  |  |

# Chapitre VAnnexes

## 5.1. Annexe 1 : Liste des contacts

### A) Internes

#### Personnes ressources

| Rôle | Prénom et NOM | Fonction | ContactsPensez à disposer de minimum 2 contacts par rôle (1 principal et 1 en cas de maladie, congé, depart du rôle principal) |
| --- | --- | --- | --- |
| Leader de l’équipe de gestion de continuité ou gestionnaire du plan de continuité |  |  | Principal @TMAutre@TM |
| Membres de l’équipe de gestion de la continuité |  |  | Principal @TMAutre@TM |
| Service fonctionnel 1 |  | Activité.s essentielle.s (identifiez) | Principal @TMAutre@TM |
| Service fonctionnel 2 |  | Activité.s essentielle.s (identifiez) | Principal @TMAutre@TM |
| … |  |  |  |

### B) Externes

#### Fournisseurs, Clients,....

| Rôle | Nom de la sociétéPrénom et NOM des contacts | Référence des contrats | ContactsPensez à disposer de minimum 2 contacts par rôle (1 principal et 1 en cas de maladie, congé, depart du rôle principal) |
| --- | --- | --- | --- |
| Fournisseur 1 |  |  | Principal @TMAutre@TM |
| Client 1  |  |  | Principal @TMAutre@TM |
| ... |  |  |  |

## 5.2. Annexe 2: Documents de référence

1. Risk Assessment et Risk Treatment
2. Gestion des incidents
3. Crisis Management Plan
4. …