

COMMUNICATION DE CRISE

 En collaboration avec :



# Communication de crise

Toute entreprise peut être confrontée à des crises. La cause de nombre de ces crises se situe en dehors de l'organisation. Souvent, des circonstances imprévues et indépendantes de votre volonté obligent votre entreprise à réagir immédiatement.

Lorsqu'une crise survient, la panique peut rapidement et facilement s'installer. Vous pouvez éviter cela en vous préparant et en disposant d'un plan de communication de crise qui décrit la manière dont vous pouvez faire face à la situation. Pour la réputation de votre organisation, ce qui compte le plus souvent c'est la façon dont vous gérez la crise qui est déterminante, et non la crise elle-même.

**Avertissement**

Les informations fournies par le présent document sont destinées à fournir des éléments de réflexion à l’employeur dans le cadre d’une gestion des incidents afin d'assurer la continuité des activités de l'entreprise. L’objectif n’est donc pas de se substituer aux autorités chargées de surveiller la sécurité du travail. Ces informations ne dispensent pas l’employeur de respecter les dispositions réglementaires qui sont susceptibles de s’appliquer pour chaque situation de travail spécifique.

Cela signifie que l’utilisation du présent document par l’employeur est toujours tributaire de son jugement pragmatique et qu’il lui appartient d’apprécier les éléments et les circonstances, en fait et en droit, auxquels l’employeur doit faire face dans les cas bien définis et concrets sur les lieux de travail.

*Pour en savoir plus sur les différentes étapes, voir template “Gestion des incidents”, Chapitre III.*

*.*

COMMUNICATION DE CRISE

[I. Etape 1 : Préparation (AVANT INCIDENT) 4](#_Toc57830296)

[1.1 : Placez un pilote dans l’avion 4](#_Toc57830297)

[1.2 : Connaissez vos risques 4](#_Toc57830298)

[1.3 : Mesures preventives 5](#_Toc57830299)

[II. Etape 2 : Notification et identification 10](#_Toc57830300)

[2.1 : Notification 10](#_Toc57830301)

[2.2 : Identification 10](#_Toc57830302)

[III. Etape 3 : Activation et traitement (INCIDENT) 12](#_Toc57830303)

[3.1 : Identifiez vos outils et moyens 12](#_Toc57830304)

[3.2 : **MESURES DE GESTION** 14](#_Toc57830305)

[IV. Etape 4 : Eradication 15](#_Toc57830308)

[V. Etape 5 : Désactivation 15](#_Toc57830309)

[VI. Etape 6 : Leçons acquises (post incident review) (APRES INCIDENT) 16](#_Toc57830310)

[6.1 : Contexte : informations relatives a l’incident 16](#_Toc57830311)

[6.2 : Evaluation de l’incident et leçons acquises 16](#_Toc57830312)

[VII. Annexes 20](#_Toc57830313)

[7.1 : Liste des contacts 20](#_Toc57830314)

[7.2 : Tableau 22](#_Toc57830315)

1. Etape 1 : Préparation (AVANT INCIDENT)

Voir également Risk Assessment et Risk Treatment.

* 1. : Placez un pilote dans l’avion

|  |
| --- |
| Qui peut dresser ce plan de gestion des incidents ?  Qui peut élaborer et gérer cette fiche ? |

*Voir Annexe VII, 7.2 : Tableau*

Dans les grandes structures, un groupe (idéalement pluridisciplinaire et inclusif) peut être constitué.

Dans les plus petites structures, il est possible qu’une seule et même personne soit désignée par la direction ou que la direction assume ce rôle elle-même. Dans ce cas, il est néanmoins conseillé de désigner un back up (une personne qui pourra le remplacer en cas d’absence, de maladie ou de départ).

Assurez-vous de faire valider les procédures/le plan de gestion des incidents ainsi que la présente fiche.

1.2 : Connaissez vos risques

|  |
| --- |
| Avez-vous réalisé un Risk Assessment ?  Avez-vous réalisé un Risk Treatment ? |

*Voir Annexe VII, 7.2 : Tableau*

Pour que le plan de gestion des incidents puisse être efficace, l’entreprise doit avoir identifié, analysé et évalué ses risques. C’est l’objet du Risk Assessment (voir template). Il faut également que les mesures de traitement des risques soient connues, c’est l’objet du Risk Treatment (voir template).

Il vous faut également identifier les scenarios spécifiques.

Il existe **trois types de crises,** selon les causes de la crise et la manière dont celle-ci affecte la réputation de l'organisation. Il est important de savoir que la menace pour la réputation de l'organisation dépend souvent des crises précédentes et de l'image existante de l'organisation concernée.

**Scenariis :**

1. **Crise “victime”**

Une crise “victime” se produit lorsque l'organisation est considérée comme une victime de la crise. Un exemple courant est celui d'une catastrophe naturelle. Si, par exemple, un incendie détruit l'infrastructure physique d'une entreprise, celle-ci ne peut plus faire des affaires. Dans ce cas, la réputation de l'organisation n'est pas ou peu affectée, car la situation est inévitable et l'entreprise ne peut pas l'empêcher.

1. **Crise “accidentelle”**

En cas de crise “accidentelle”, c'est l'organisation qui est responsable, mais ses actions n'étaient pas intentionnelles. Même lorsque ce type de crise semble insignifiant, il est important de s'y attaquer rapidement avant que la situation n'ait le temps de s'aggraver.

1. **Crise “évitable”**

Lorsque l'organisation prend un risque calculé qui conduit à un résultat ou un événement négatif, on parle de "crise évitable". Ce type de crise constitue une menace majeure pour une organisation car sa réputation est en jeu. Dans une telle situation, les réponses et les actions de l'organisation face à la crise sont cruciales. Malgré ces mesures, il est extrêmement difficile de reconstruire la réputation de votre marque après une telle crise.

### 1.3 : Mesures préventives

Dans les trois scénarios ci-dessus, il existe différentes stratégies de réponse que les entreprises peuvent utiliser pour faire face à un incident/crise. Il importe de savoir qui est responsable de la crise et de déterminer l'ampleur de la menace qui pèse sur la réputation de l'entreprise.

Plus précisément, il existe quatre grandes stratégies de communication :

1. **Stratégie de reconstruction**

Cette stratégie vise à reconstruire les relations avec les parties prenantes en rétablissant la réputation de l'organisation. Pour ce faire, il faut assumer la responsabilité de la crise et présenter des excuses aux personnes touchées par son issue.

1. **Stratégie de confinement**

Cette stratégie fonctionne en minimisant le degré de responsabilité de l'organisation. Pour ce faire, il faut présenter des excuses ou justifier les actions de l'entreprise.

1. **Stratégie de refus**

Cette stratégie élimine complètement le blâme de l'organisation. Pour ce faire, on confronte le ou les "accusateurs" à leurs accusations non fondées, en prétendant qu'il n'y a pas de crise, ou en rejetant la responsabilité de la crise sur une autre partie.

1. **Stratégie de soutien**

Cette stratégie fonctionne en positionnant l'organisation comme un atout pour ses stakeholders (fournisseurs, clients,...) et en leur rappelant ses bonnes actions passées. En outre, les stakeholders sont félicités et remerciés pour leur dévouement et leur loyauté. Une stratégie de soutien est souvent utilisée en combinaison avec d'autres stratégies de crise primaires (voir tableau, Chapitre III., 3.1 Identifiez vos outils et vos moyens).

**Autres conseils et astuces :**

* Sensibilisation interne : s'assurer que chacun au sein de l'entreprise comprend l'importance d'une bonne information en cas de crise.
* Mise en place d'une chaine de réaction face à une crise (incident majeur) : qui sont les personnes concernées et quelles sont leurs responsabilités ?
* Pratiquez différentes situations de crise par le biais de jeux de rôle.
* Élaborer un plan de gestion de crise ou un plan de gestion des incidents et le mettre à jour chaque année.
* Établir une coopération naturelle avec les autorités nécessaires.

Quelle que soit la stratégie adoptée, pensez notamment à:

1. DÉFINIR L'INCIDENT.

* Que se passe-t-il ? Quel incident s'est produit ? Quelle en est la cause ?

1. ANALYSER L'INCIDENT.

* Quelle est la gravité de la situation ? Y a-t-il un impact sur les processus commerciaux essentiels ?

1. DÉFINIR LA SOLUTION.

* Comment résoudre l'incident ? Que faut-il faire ?
* Que faut-il faire en premier lieu ? Définissez vos priorités !

1. IDENTIFIER RÉPARTITION DES TÂCHES ET DES RESPONSABILITÉS.

* Le gestionnaire de crise détermine qui doit faire quoi. Informez également le personnel en interne concernant l'évolution de la situation.

1. COMMUNIQUER À L'EXTÉRIEUR.
   * Contacter les organismes nécessaires (par exemple, les autorités, les services publics, etc. Si nécessaire, informez également les clients, les fournisseurs et les autres parties prenantes (stakeholders).
2. ASSURER LE SUIVI.
   * Une fois l'incident résolu, effectuer un post incident review à cette fin :

A) Comment mieux traiter cet incident à l'avenir &

B) Comment pouvons-nous éviter cet incident à l'avenir ?

Pour pouvoir communiquer rapidement et efficacement en situation de crise, il faut **une structure logique dans les rapports**. De cette façon, vous n'oubliez pas les informations importantes et vous communiquez avec précision. Les exemples ci-dessous sont un guide, mais devront bien sûr être adaptés à vos besoins spécifiques et aux canaux de communication disponibles.

|  |
| --- |
| **Élément 1 : Que s'est-il passé exactement ?** |
| Message : Décrivez brièvement et de façon factuelle la situation. Restez objectif et ne devinez pas les raisons ou les causes si elles ne sont pas encore connues. |

|  |
| --- |
| **Élément 2 : Quel est l'impact pour votre groupe cible ?** |
| Message : Quelles sont les conséquences pour votre groupe cible en ce moment ? |

|  |
| --- |
| **Élément 3 : Que font les services /la gestion /les organisations associées ?** |
| Message : Que se passe-t-il pour maîtriser la situation ou rétablir une situation normale, quelles sont les prochaines étapes ? |

|  |
| --- |
| **Élément 4a : Que doit faire le groupe cible ?** |
| Message : Précisez brièvement ce qui est attendu du groupe cible. |

|  |
| --- |
| **Élément 4b: Quel comportement n’est pas encouragé pour le groupe cible ?** |
| Message : Indiquez brièvement les actions que vous souhaitez éviter et délimitez les responsabilités le cas échéant. |

|  |
| --- |
| **Élément 5 : Où le groupe cible pourra-t-il trouver plus d'informations ?** |
| Message : Qui est la personne de contact au sein de l'entreprise qui coordonne cette crise ? Par quels canaux le groupe cible sera-t-il tenu informé et où pourra-t-il poser ses questions ? |

|  |
| --- |
| **Élément 6 : Quand en le groupe cible pourra-t-il en savoir plus ?** |
| Message : Faites une estimation du moment où une prochaine communication suivra et par quels canaux. |

Pour vous aider, voici deux exemples de communication : une communication interne et une communication externe.

#### 1.3.1 : Communication interne

*Exemple d’une fraude CEO, Appel à la vigilance*

*Bonjour à toutes,*

*Aujourd'hui, certaines d'entre vous ont reçu le courrier ci-dessous.*

*Afbeelding met tekst

Automatisch gegenereerde beschrijvingATTENTION : Il s'agit d'une* ***fraude "CEO",*** *c'est-à-dire une technique par laquelle des escrocs se font passer pour notre CEO.*

*Ne répondez pas à ce mail frauduleux !*

*Réfléchissez toujours avec soin lorsque vous recevez un tel courrier.*

*Tout d'abord, vérifiez l'adresse électronique. Cela semble souvent correct à première vue, mais en y regardant de plus près, il s'avère qu'il s'agit d'une adresse externe. (Conseil : passez votre curseur sur l'expéditeur pour voir l'adresse sous-jacente). Demandez-vous toujours si ce qui est demandé dans le courriel est conforme aux procédures applicables.*

*Si un membre de la direction vous demande d'effectuer un paiement alors que cela ne fait normalement pas partie de vos fonctions, ou s'il vous demande de ne pas en parler à quelqu'un d'autre, vérifiez toujours par un autre canal si la demande est bien réelle et provient bien de la personne autorisée !*

*Vous trouverez également en pièce jointe à ce courrier les fiches d'information (sur le phishing et la fraude CEO avec plus d'informations.*

*Pour toute question complémentaire, vous pouvez toujours contacter Pierre Quiroule ou le service informatique.*

*Merci pour votre coopération,*

*Tom.B. Padanlpano,*

*Officemanager*

#### 1.3.2 : Communication externe

*Exemple de fuite d’eau et bâtiment inaccessibles*

*Cher client,*

*En raison des pluies exceptionnellement abondantes de la nuit dernière, l’eau a fui dans le 1er étage du bâtiment de <Nom d’entreprise>. Une partie du plafond s’est effondrée. La salle des serveurs est protégée, mais la plupart des bureaux ne sont plus utilisables à cause de l’effondrement du plafond et de l’eau présente.*

*Par conséquent, l’immeuble de l’entreprise n’est actuellement PAS accessible aux clients et au personnel.*

*Le service des pompiers inspectera le bâtiment ce matin, après quoi un toiturier effectuera les premières réparations.*

*Notre personnel travaillera donc à domicile pour le moment, vos contacts réguliers resteront disponibles par e-mail et téléphone mobile. Notre boutique en ligne sera également accessible via www.Nomd’entreprise.be. Les livraisons prévues ne seront en principe pas affectées par cette fuite d’eau.*

*Nous vous tiendrons bien entendu informés de l’évolution de la situation. Une mise à jour de la situation suivra demain matin par mail. Pour toute question urgente, veuillez contacter le numéro 04 xxx xx xx.*

*En vous remerciant pour votre compréhension,*

*O. Waterfall*

1. Etape 2 : Notification et Identification

### 2.1 : Notification

Il est essentiel de pouvoir détecter, identifier et qualifier/classer rapidement un incident afin d’en limiter l’impact sur la continuité des activités en activant la procédure adéquate. La personne qui reçoit la notification de l’incident qualifie l’incident sur base de critères prédéterminés.

Chaque employé doit signaler tout incident ou événement susceptible d’entraîner un incident, et ce dès que possible. Les clients et fournisseurs peuvent également signaler un incident.

Les moyens de signaler les incidents sont décrits dans le processus de gestion des incidents.

* Voir Etape 3. Activation et Traitement, Mesures de gestion

### 2.2 : Identification

2.2.1 : Identifiez les activités concernées

|  |
| --- |
| Quelles sont les tâches de l’entreprise qui doivent être maintenues pour assurer sa survie économique ?  Voir également le plan de gestion des activités (Business Continuity plan - BCP) et les objectifs de temps fixes (RTO,...) |

Pour vous aider à identifier les processus et activités prioritaires, posez-vous les questions suivantes:

1. quelles sont les activités qui peuvent mettre en danger le personnel (ou les clients) ?
2. quelles sont les activités qui après quelques heures auraient un impact économique significatif pour votre entreprise ? Après 24h ? 45h ? Une semaine ?

LISTE DES ACTIVITES ESSENTIELLES

| **Activité essentielle 1** |
| --- |
| Liste des éléments nécessaires pour la continuité de l’activité essentielle |
| Personnel clef |
| Information ou données clefs |
| Service informatique (hardware, software) nécessaire |
| Bâtiments |
| Personnes externes de contact (ressources) |
| Interdépendance avec d’autres activités (si oui, lesquelles) |
| ... |

2.2.2 : Classez

La personne qui reçoit les renseignements (p. ex. Helpdesk) doit les classer, par exemple de la manière suivante:

1. **Faible** – aucun incident ne s’est produit, mais l’événement lié à un système, à un processus ou à une organisation peut déclencher la survenance d’un incident dans un avenir proche ou ultérieur;
2. **Mineur** – incident qui n’a pas d’impact significatif sur la continuité des activités;
3. **Majeur** – incident qui peut avoir un impact significatif sur l’organisation, mais qui n’est pas encore considéré comme une crise;
4. **Crise** – incident qui peut avoir un impact significatif sur l’organisation et la continuité des activités.

2.2.3 : Identifiez les priorités

|  |
| --- |
| En cas d’interruption ou de dégradation de vos activités, quel est l’ordre de priorité des activités ?  Quels sont vos objectifs de temps ?  Voir également les Risk Assessment, Risk Treatment et plan de continuité des activités |

Lors de l’analyse relative à l’impact sur la continuité des activités, gardez à l’esprit qu’il est possible que toutes les activités ne fonctionnement pas forcément à 100% et que cela puisse être acceptable.

Vous avez défini vos activités essentielles impactées ? Il s’agit maintenant d’identifier l’ordre dans lequel ces activités devraient reprendre (certains services sont interdépendants des autres) et d’identifier les objectifs de temps estimé en les comparant aux objectifs fixés (voir Risk Assessment et Business Continuity Plan).

En fonction de ce qui précède, identifiez l’ordre dans lequel les actions doivent être entreprises afin d’assurer la continuité des activités essentielles. N’oubliez pas d’envisager l’interdépendance possible de certaines activités et de maintenir un dialogue constant avec le gestionnaire du plan de continuité des activités.

1. Etape 3 : Activation et Traitement (INCIDENT)

### 3.1 : Identifiez vos outils et moyens

*Voir annexe VII, point 7.2 : Tableau*

En particulier, vos procédures (identification...), vos moyens de communication...

L’objectif principal est de réduire aussi rapidement que possible l’impact de l’incident pour la protection de la vie humaine puis pour la continuité des activités de l’entreprise.

Quelle stratégie adopter en cas de crise ? Vous le trouverez dans les tableaux ci-dessous, subdivisés en stratégies de réponse aux crises primaires et secondaires :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type de**  **stratégie** | **Type de crise** | **Stratégie de réponse** | **Action tactique** | **Description de l'action tactique** |
| Stratégies de réponse primaires | Crise victime | Stratégie de refus | Y aller de front | Confrontez la personne/le groupe qui prétend que quelque chose ne va pas. |
| Nier | Prétendez qu'il n'y a pas de crise. |
| Trouver un bouc émissaire | Blâmez une personne ou un groupe extérieur à l'organisation pour la crise. |
| Crise accidentelle | Stratégie de confinement | Justifier | Réduisez votre responsabilité en :   * niant que vous aviez l'intention de causer un préjudice ; * en faisant valoir que vous ne pouvez pas contrôler la cause de la crise. |
| S'excuser | Minimisez les dommages causés par la crise. |
| Crise évitable | Stratégie de reconstruction | Compenser | Offrez une compensation (par exemple de l'argent ou d'autres cadeaux) aux victimes de la crise. |
| Assumer | Assumez pleinement la responsabilité de la crise et demandez pardon. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Type de stratégie** | **Stratégie de réponse** | **Action tactique** | **Beschrijving v/d tactische actie** |
| Stratégies de réponse secondaires | Stratégie de reconstruction | Faire appel à l'histoire | Rappelez aux/Informez les parties prenantes les précieuses réalisations passées de l'organisation. |
| Flatter | Félicitez les parties prenantes et leur rappeler les précieuses réalisations passées de l'organisation. |
| Etre reconnu comme "victime" | Rappelez aux parties prenantes que l'organisation est également victime de la crise. |



#### **3.2 : MESURES DE GESTION**

|  |  |
| --- | --- |
|  | **DO’s** |
|  | **Communiquez d'abord en interne** (ses propres employés) et à tous les acteurs concernés (parties prenantes, partenaires, partenaires-citoyens...), puis seulement à l'extérieur. |
|  | **Limitez-vous aux faits.** Assurez-vous que vos informations sont correctes et aussi complètes que possible. |
|  | Diffusez le message par **différents canaux**. Vous augmentez les chances que les gens entendent et acceptent plus rapidement votre message et vous limitez les risques qu’ils se retrouvent “coincés”. |
|  | La façon dont vous communiquez avec le personnel, les parties prenantes, la presse... dépend de la **nature de la crise**. C’est le moment de sortir vos messages préparés et de les adapter ! |
|  | **Rassurez les gens et donnez-leur des conseils.** |

|  |  |
| --- | --- |
|  | **DONT’S** |
|  | **Ne vous laissez pas prendre au piège de la vitesse.** Plus vous communiquez rapidement, moins vous laissez de place à la spéculation et aux coups de bâton. Mais une réaction rapide n'est pas à confondre avec une réaction émotionnelle ou improvisée. |
|  | **N'oubliez aucun groupe cible :** pensez aussi à la presse, aux autres parties concernées, aux tiers intéressés tels que les voisins,... |
|  | Ne traitez pas l'incident de manière professionnelle et sans émotion. **Mais ne laissez pas les émotions prendre le dessus.** |
|  | **Ne répondez jamais immédiatement aux journalistes par téléphone. Laissez quelqu'un répondre au téléphone, notez les coordonnées du journaliste et ce qu'il veut savoir. Rappelez un quart d'heure plus tard et préparez-vous.** |
|  | **Soyez ouvert et honnête, mais ne révélez pas tous les détails.** Respectez toujours l'intégrité et la vie privée des personnes concernées. Ne divulguez PAS d'informations confidentielles. |

1. Etape 4 : Eradication

Il n’est pas toujours possible de déterminer pendant l’incident les causes de celui-ci. Dans ce cas, il s‘agira d’abord d’agir sur les conséquences (impact sur la continuité des activités) avant de pouvoir en déterminer la cause. Toutefois, des efforts raisonnables doivent être déployés pour pouvoir identifier la cause et limiter les risques qu’un tel incident se reproduise à nouveau...

1. Etape 5 : Désactivation

Lorsque les services touchés par un incident sont revenus à des opérations normales, l’incident peut être clos par l’équipe de gestion de l’incident (p.ex. helpdesk) en accord avec le gestionnaire du Business Continuity Plan.

Le plan de gestion des incidents est désactivé et un “post incident review” est effectué (voir étape 6).

Les mesures suivantes devraient être prises:

| **Action** | **Fonction** | **Liens vers d’autres documents**  **Nom et référence** |
| --- | --- | --- |
| Fermer le ticket d’incident | Helpdesk après accord du gestionnaire du plan de gestion des incidents | Ticket dans le cadre de l’Incident Management |
| Désactiver le plan de gestion des incidents | Gestionnaire du plan des incidents |  |
| Effectuer le Post Incident Review | Gestionnaire du plan des incidents | Post Incident Review (document) |
| … |  |  |

1. Etape 6 : Leçons acquises (Post Incident Review) (APRES INCIDENT)

*“I never lose. I either win or learn.”*

Nelson Mandela

Il s’agit d’apprendre de son expérience en réalisant un “post incident review” afin d’améliorer dans un processus continu la gestion des incidents.

Le Post Incident Review devrait comprendre au moins les éléments suivants :

6.1 : Contexte : Informations relatives a l’incident

| **Élément** | **Information** |
| --- | --- |
| **Administration** |  |
| Numéro de l’incident dans le registre des incidents: |  |
| Date et heure de la détection de l’incident: |  |
| Date et heure de la résolution de l’incident: |  |
| Type d’incident: |  |
| Gravité de l’incident: |  |
| Les clients ont-ils été touchés: |  |
| Gestionnaire de l’incident: |  |
| Description de l’incident: |  |
| ... |  |

6.2 : Evaluation de l’incident et leçons acquises

|  |  |
| --- | --- |
| **Détection** |  |
| Comment et par qui l’incident a-t-il été détecté: |  |
| L'incident a-t-il été détecté rapidement ou aurait-il pu l'être plus tôt: |  |
| Peut-on utiliser des procédures ou des outils pour détecter les incidents plus tôt? |  |
| Les procédures de notification des incidents ont-elles été suivies: |  |
| **…** |  |
| **Evaluation et actions** |  |
| L'incident a-t-il été évalué correctement et correctement ?  L’information appropriée était-elle disponible pour ce faire : |  |
| Le BCP a-t-il été activé ? |  |
| Quelles autres mesures ont été prises pour résoudre l’incident: |  |
| Quelles ressources ont été utilisées pour gérer l’incident: |  |
| Le plan est-il suffisamment souple pour faire face à des événements imprévus: |  |
| Les mesures ont-elles été prises en temps opportun? |  |
| **…** |  |

|  |  |
| --- | --- |
| **Communication** |  |
| Une communication interne a-t-elle été envoyée (en temps voulu): |  |
| La communication externe a-t-elle été envoyée (en temps voulu): |  |
| Quels médias ont été utilisés: |  |
| Quand la première communication a-t-elle été envoyée et quelle fréquence de mise à jour a-t-elle été utilisée? |  |
| Les personnes concernées ont-elles été impliquées: |  |
| Quelles sont les communications utiles: |  |
| Quelles communications ont été employées et se sont révélées inefficaces : |  |
| **…** |  |

|  |  |
| --- | --- |
| **Prévention** |  |
| Que peut-on apprendre de ce qui s’est passé: |  |
| Comment éviter la répétition d’incidents, quelles mesures peuvent être prises pour le faire et qui est responsable de leur exécution: |  |
| **…** |  |

|  |  |
| --- | --- |
| **Analyse des causes profondes** |  |
| La cause de l’incident a-t-elle été détectée: |  |
| Incidents liés ou de nature similaire: |  |
| Y a-t-il un problème sous-jacent: |  |
| Le problème sous-jacent a-t-il été détecté (voir étape 4 Eradication) |  |
| **…** |  |

|  |  |
| --- | --- |
| **Adéquation de la réponse** |  |
| Temps réel de récupération (comparez avec le Recovery Time Objective RTO)  L’incident a été résolu dans le délai prédéterminé:  Pour aucune des activités  Seulement pour quelques activités  Pour toutes les activités |  |
| Faut-il réadapter les contrats ? |  |
| … |  |

|  |  |
| --- | --- |
| **Pertinence de la réponse du management à l’incident** |  |
| Le management n'a pas répondu ou n'a pas répondu de manière satisfaisante. |  |
| Le management a répondu, mais n’a pas suivi complètement les plans. |  |
| Le management a répondu pleinement conformément aux plans. |  |
| **…** |  |

|  |  |
| --- | --- |
| **Niveau de préparation du personnel** |  |
| 1. Non préparé |  |
| 2. Partiellement préparé |  |
| 3. Entièrement préparé |  |
| … |  |

|  |  |
| --- | --- |
| **Améliorations souhaitées** |  |
| Quels éléments pourraient être ajustés: |  |
| … |  |

|  |  |
| --- | --- |
| **Dommages et intérêts** |  |
| Y a-t-il des demandes de dommages-intérêts: |  |
| Des demandes de dommages-intérêts ont été déposées auprès de tiers dans le cadre de cet incident: |  |
|  |  |

|  |  |
| --- | --- |
| **Divers** |  |
| ... |  |

1. Annexes

7.1 : Liste des contacts

**INTERNES**

| **Fonction** | **Prénom NOM**  ***Pensez à designer une autre personne en cas d’absence, maladie,... de la personne de référence.*** | **Actions** | **Coordonnées**  ***Téléphonie fixe***  ***Bureau***  ***Maison***  ***Mobile***  ***Email***  ***Préférences de contact (le + rapide)*** |
| --- | --- | --- | --- |
| Personne de référence (continuité des activités) |  |  |  |
| Suppléant |  |  |  |
| ... |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**EXTERNES**

| **Fonction** | **Prénom NOM**  ***Pensez à designer une autre personne en cas d’absence, maladie,... de la personne de référence.*** | **Contrats**  ***Référence*** | **Coordonnées**  ***Téléphonie fixe***  ***Bureau***  ***Maison***  ***Mobile***  ***Email***  ***Préférences de contact (le + rapide)*** |
| --- | --- | --- | --- |
|  |  |  |  |
| Journalistes |  |  | Téléphone fixe  Bureau  1)  2)  Maison  1)  2)  Mobile  1)  2)  Email  1)  2) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| … |  |  |  |
| … |  |  |  |

* 1. : Tableau

|  |  |  |
| --- | --- | --- |
| **1.1 Placez un pilote dans l’avion** | **Qui accomplit la tâche** | **Quelles procédures faut-il suivre?** |
|
| [Scenario 1] |  |  |
| [Scenario 2] |  |  |
| […] |  |  |

|  |  |  |
| --- | --- | --- |
| **1.2: Connaissez vos risques** | **Prendre le résultat de la colonne P de votre Risk Assessment (2 (vert) à 10 (rouge)** | **Groupe Focus ?** **(1 ou 2)** |
| Dans votre Risk Assessment, quel est votre niveau de risque pour le scénario 1? |  |  |
| Dans votre Risk Assessment, quel est votre niveau de risque pour le scénario 2 |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  | **2.2.3: Identifiez les priorités**   * Quels sont vos objectifs de temps? * Quel est le délai maximum «acceptable» pour restaurer l’activité? (Recovery Time Objective, RTO) * Quel est l’âge maximum des données dont vous avez besoin pour récupérer (Recovery Point Objective, RPO) * Qu’avez-vous prévu avec vos fournisseurs (Recovery Consistency Objective, RCO)? * ... en cas d’interruption ou de détérioration de vos activités, quel est l’ordre de priorité des activités (P)? | | | |
| **2.2.1 Identifiez les activités concernées (Scenario 1)** |  | | **RTO** | **RPO** | **RCO** | **P** |
| Ressources humaines |  | |  |  |  |  |
| Infrastructures |  | |  |  |  |  |
| Technologie |  | |  |  |  |  |
| Information et documentation |  | |  |  |  |  |
| Tiers |  | |  |  |  |  |
| **…** |  | |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| **3.1: Identifiez vos moyens et outils (Scenario 1)** | **Activité essentielle 1** | **Activité essentielle 2** |
| Personnel clef |  |  |
| Informations ou données importantes |  |  |
| Services informatiques nécessaires (matériel, logiciel) |  |  |
| Bâtiments |  |  |
| Contacts externes (ressources) |  |  |
| Interdépendance avec d'autres activités (si oui, qui) |  |  |
| **…** |  |  |