

FRAUDE CEO

CATEGORIE: IT (malware)

 En collaboration avec :



# Fraude CEO

**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 des interprétations lors de cas ou de situations concrètes, l'avis des fonctionnaires chargés de surveiller la réglementation relative à la sécurité du travail peut toujours être sollicité.

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

**Fraude CEO**

[I. Etape 1: Préparation (AVANT INCIDENT) 4](#_Toc57560655)

[1.1 : Placez un pilote dans l’avion 4](#_Toc57560656)

[1.2 : Connaissez vos risques 4](#_Toc57560657)

[1.3 : Mesures préventives 6](#_Toc57560658)

[II. Etape 2 : Notification et Identification 9](#_Toc57560659)

[2.1 : Notification 10](#_Toc57560660)

[2.2 : Identification 10](#_Toc57560661)

[III. Etape 3: Activation et Traitement (INCIDENT) 11](#_Toc57560662)

[3.1 : Identifiez vos outils et moyens 11](#_Toc57560663)

[3.2 : **MESURES DE GESTION** 12](#_Toc57560664)

[IV. Etape 4 : Eradication 13](#_Toc57560665)

[V. Etape 5 : Désactivation 13](#_Toc57560666)

[VI. Etape 6 : Leçons acquises (Post Incident Review) (APRES INCIDENT) 13](#_Toc57560667)

[6.1 : Contexte : Informations relatives a l’incident 14](#_Toc57560668)

[6.2 : Evaluation de l’incident et leçons acquises 14](#_Toc57560669)

[VII. Annexes 18](#_Toc57560670)

[7.1 : Liste des contacts 18](#_Toc57560671)

[7.2 : Tableau 19](#_Toc57560672)

1. Etape 1 : Préparation (AVANT INCIDENT)

Voir également Risk Assessment et Risk Treatment.

### 1.1 : 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).

Pensez à inclure votre service informatique (interne ou externe) si vous en disposez.

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

|  |
| --- |
| Avez-vous réalisé un risk assessment ?  Avez-vous réalisé un Risk Treatment ? |

### 1.2 : Connaissez vos risques

*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).

Vous devez également identifier des scénarios spécifiques.

**Scénario :**

La fraude CEO (PDG) est une forme d'hameçonnage (phishing) plus sophistiquée et plus rusée (elle relève de la famille des "spear phishing"). Dans ce cas, le hameçonneur a d'abord étudié l'entreprise en profondeur et il sait dans une certaine mesure comment l'entreprise est organisée et fonctionne. Il se fait alors passer pour le CEO (ou une personne ayant une position d'autorité) et contacte des personnes spécifiques au sein de l'entreprise via une adresse électronique fausse ou piratée (ou par téléphone) dans le but de transférer de l'argent en urgence ou de communiquer des données sensibles. Ainsi, les contrôleurs financiers sont souvent la cible de la fraude CEO, mais le personnel de la presse ou les services informatiques peuvent également en être victimes, voire d'autres cadres supérieurs ! Ce dernier cas est parfois appelé "Whale phising" : on tente d'attirer une "baleine" dans un piège au lieu d'un petit poisson.

Un employé inattentif pense qu'il a été contacté par CEO de l'entreprise pour laquelle il travaille et face à la position d'autorité, il obéit et effectue la mission sans se douter de rien.

**DE :** Le Grand Chef < lebigboss@votrecompagnie.com >

**Envoyé le :** 09 octobre 2020 11:06

**A :** Le service comptable de votre entreprise <jean.dupuis@votrecompagnie.com>

**Objet :** URGENT : Paiement à exécuter sans tarder

Bonjour Jean,

Pourrais-tu me faire une faveur stp ? Je viens de recevoir un rappel de l'un de nos fournisseurs qui m'indique que nous sommes en retard de paiement et qu'il appliquera des sanctions si l'entreprise ne paie pas aujourd'hui. Comme je suis en réunion extérieure toute la journée aujourd'hui, je serai injoignable et je peux pas m'en occuper d'ici. Pourrais-tu rapidement faire le nécessaire stp ? Je leur ai dit de t'envoyer un mail directement (entreprise XX). N'oublie pas de vérifier tes indésirables au cas où !) sinon tu peux payer en cliquant sur le lien ici et transférer le montant indiqué.

Cela doit être fait en priorité AUJOURD'HUI.

Je sais que je peux compter sur toi.

Si tu as la moindre question, tu peux répondre via ce mail car comme indiqué, je ne serai pas joinable par téléphone aujourd'hui...

Merci,

Le CEO

**Risques** :

Il y a généralement une perte financière, mais il peut aussi y avoir une perte de données personnelles ou d'entreprise, une atteinte à la réputation,... Bien que moins courants, des logiciels malveillants peuvent également être installés.

### 1.3 : Mesures préventives

#### Techniques

Bien que la fraude CEO soit une forme d'hameçonnage (phishing) plus sophistiquée, les mêmes mécanismes de défense techniques peuvent être également être utiles dans ce cas précis.

Demandez toujours conseil à votre responsable informatique (interne ou externe), si votre entreprise en dispose. Ils peuvent vous aider en vous donnant des conseils sur les applications techniques utiles que vous pouvez utiliser pour défendre votre entreprise.

Vous trouverez ci-dessous quelques bonnes pratiques :

* Utilisez une **passerelle de messagerie électronique sécurisée** ("SEG").
* Les courriers électroniques entrants et sortants sont filtrés pour détecter le phishing, le spam, les logiciels malveillants, ... Cela réduit considérablement le risque qu'un courrier électronique de phishing se retrouve encore dans la boîte de réception. Certains fournisseurs connus sont cisco, IBM, citrix, ...
* Désactivez **l'affichage de l'aperçu** des pièces jointes et l'affichage des images.
* Les pièces jointes et les images peuvent être nuisibles ! Ce n'est pas parce qu'un e-mail contient des images qu'elles se trouvent réellement dans cet e-mail : une image ne fait pas toujours automatiquement partie d'un e-mail, elle est généralement téléchargée via un lien caché (URL). Ces liens cachés peuvent être autant de portes d'entrée pour vous des cyberattaquants. Par ailleurs, en téléchargeant une image, vous indiquez également à l'attaquant que l'adresse électronique est toujours utilisée : vous pouvez donc vous attendre à recevoir encore plus de messages de phishing ou de spam.
* Mettez en place **une politique de mots de passe forts** ou mieux encore : utilisez une **authentification** **multifactorielle** (Multi-Factor Authentification MFA) pour vous connecter à vos comptes et systèmes d'information.
* Au lieu d'utiliser simplement un (login) nom de connexion et un mot de passe, vous pouvez demander à installer des facteurs supplémentaires pour vous connecter. Vous pourriez par exemple prévoir d'envoyer une confirmation par sms depuis un numéro de téléphone de confiance, ou accepter l'utilisation de données biométriques telles que les empreintes digitales ou la reconnaissance faciale. Un exemple bien connu est celui de "[Itsme](https://www.itsme.be/)". En utilisant l'authentification à plusieurs facteurs, vous réduisez les chances qu'un hameçonneur (phisher) qui pourrait avoir votre mot de passe, puisse l'utiliser car il ne disposera pas des autres facteurs.

**Comme toujours, tenez compte des règles de base suivantes pour une bonne cyberhygiène :**

#### Organisationnelles

Tout comme une attaque de phishing normale, la fraude CEO ne peut réussir que si certaines personnes tombent réellement dans le piège. Cependant, dans le cas de la fraude CEO, il est beaucoup plus difficile de voir d'un seul coup d'œil que quelque chose ne va pas, car le fraudeur s'est soigneusement préparé pour paraître crédible. **Sensibiliser et tester tous les employés est donc essentiel ici aussi !** Une attention particulière doit être accordée au niveau de la direction, non seulement parce qu'elle est une cible potentielle, mais aussi parce que c'est souvent en son nom que la fraude CEO aura lieu. Chaque employé devrait pouvoir regarder un e-mail d'un œil critique et ne pas se contenter de suivre aveuglément des missions étranges et inattendues. (voir également fiche Phishing).

La fraude CEO est plus rusée que l'attaque phishing ordinaire. Souvent, il n'y aura pas de fautes d'orthographe et le fraudeur se fera également passer pour une personne connue au sein de l'entreprise en abusant de son autorité.

**Néanmoins, il y a quelques caractéristiques typiques** :

* Le message reste urgent
  + L'argent doit être transféré rapidement ou des informations sensibles doivent être divulguées, de préférence dès aujourd'hui.
* La mission est contraire aux procédures internes établies
  + Dans la plupart des cas, la mission doit rester confidentielle : il s'agit d'une surprise, d'un projet secret prestigieux, d'un projet aux difficultés cachées,...
* Le CEO (PDG ou toute autre personne en autorité) déclare qu'il se trouve être bloqué dans une réunion ou qu'il n'est pas présent à un bureau et ne peut pas le faire lui-même.
  + Le CEO compte spécifiquement sur vous pour mener à bien la mission et fait pression sur vous
  + Vous rendriez un grand service au CEO ou vice versa : risque de sanctions si vous ne donnez pas suite à l'ordre.
  + Il vous sera demandé de ne pas passer d'appel téléphonique et de ne répondre qu'à l'adresse électronique utilisée (ou de ne pas répondre du tout).
* Le CEO indique qu'un fournisseur de confiance doit être payé, mais le paiement doit être effectué sur un nouveau numéro de compte bancaire.
  + Le CEO indique qu'une personne, par exemple un avocat, vous contactera par téléphone au sujet d'une question urgente.
* Le CEO ne vous a jamais contacté directement ou ne vous a jamais demandé une mission similaire.

Vérifiez l'adresse électronique !

L'adresse électronique vous paraît étrange, vous est inconnue ou a été créée avec soin. Passez le curseur de la souris sur l'adresse de l'expéditeur pour la voir en entier ! Les choses auxquelles il faut prêter attention :

* L'expéditeur semble être votre CEO, mais l'adresse électronique réelle provient de l'extérieur de l'entreprise, par exemple CEO@gmail.com, CEO@hotmail.com,... au lieu de CEO@votrecompagnie.be
* L'adresse électronique correspond parfaitement, à l'exception d'un petit changement dans le nom de domaine, par exemple CEO@votrecompanie.be (sans "g") au lieu de CEO@votrecompagnie.be ou par exemple la lettre "l" a été remplacée par une lettre "i" en majuscule.
* Mais l'adresse électronique peut aussi correspondre parfaitement
  + Parce que c'est un faux (en jargon : "spoofing"). Les réponses sont alors généralement redirigées vers une adresse électronique différente (l'adresse de réponse sera différente ici). En principe, une bonne passerelle de courrier électronique sécurisée bloque ces courriers.
  + Soit parce que l'adresse électronique réelle du CEO a été piratée, ce qui est d'autant plus inquiétant.
* Il est **normal de douter** qu'un courriel soit faux ou réel !
  + Contactez le CEO (ou ses services) directement (par d'autres canaux officiels, et non en répondant au courrier), afin d'être immédiatement sûr que le courrier est vrai ou faux.
* **Ne partagez pas les informations internes** (sécurité, procédures, organisation interne,...) avec d'autres personnes extérieures à l'entreprise (même pas sur les médias sociaux).
* Voir aussi la fiche sur le phishing pour les caractéristiques plus générales des courriers de phishing.

**Au niveau du Management (Direction), les conseils suivants peuvent être utiles :**

* Mettez en place **une politique sur les méthodes de communication** au sein de votre entreprise pour la communication officielle et l'exécution des missions.
  + Par exemple, il peut être exigé que le compte de l'entreprise soit toujours utilisé pour envoyer des courriers électroniques et que tous les courriers électroniques des employés qui envoient à partir d'une adresse électronique étrangère ne soient pas suivis.
  + Convenez aussi clairement avec les fournisseurs/clients des canaux de communication officiels. La fraude CEO ne se produit pas seulement dans l'entreprise ! Votre fournisseur/client peut également être contacté pour demander l'exécution d'une certaine mission qui s'écarte du cours normal des affaires.
* Mettre en place **une politique d'exécution des paiements**.
  + Veiller à ce que les paiements ne puissent jamais être effectués sur la base d'un simple courriel d'un supérieur hiérarchique, mais qu'ils fassent l'objet de procédures officielles et soient soumis à de multiples vérifications et approbations (en particulier pour les montants importants).
* Assurez-vous qu'il n'y a **pas de culture de la peur** au sein de l'entreprise.
  + Toute attaque ou incident doit être signalé dès que possible, sans crainte d'être jugé. Plus un incident reste longtemps sous le radar, plus les dommages potentiels peuvent être importants pour l'entreprise.
  + Envisager un point de contact central
* **Vérifiez régulièrement vos dépenses bancaires** pour vous assurer qu'aucun travail manuel suspect n'est effectué.
* Évaluez s'il pourrait être avantageux pour votre entreprise de souscrire **une cyber-assurance** pouvant couvrir les dommages éventuels.

**N'oubliez pas d'organiser des exercices réguliers**. L'acquisition et le maintien de bons réflexes nécessitent des exercices réguliers. De plus, c'est souvent grâce à ces exercices que l'entreprise se rend compte que les données ne sont plus à jour (numéros de contact qui ne sont plus valables, contrats qui ont expiré, etc....), que les nouveaux employés n'ont pas encore été formés, que le logiciel n'est pas à jour, etc....). Et pourquoi ne pas organiser un "faux phishing (hameçonnage)" ? Vous pourriez surprendre votre personnel, voir "qui intervient" et comment vous pouvez sensibiliser votre personnel. Bien entendu, l'intention n'est pas de punir ceux qui tombent dans le panneau, tout le monde peut faire une erreur, le plus important est d'apprendre et d'être conscient.e....

Liens utiles

* Reconnaître une fraude CEO: [Cert.be](https://cert.be/fr/paper/la-fraude-au-ceo-mieux-vaut-prevenir-que-payer); [Febelfin](https://www.febelfin.be/fr/dossiers/comment-prevenir-la-fraude-au-ceo); [police fédérale](https://www.police.be/5998/fr/actualites/fraude-au-ceo), [dnsbelgium](https://www.dnsbelgium.be/fr/nouvelles/attention-la-fraude-au-ceo)
* Phishing herkennen: [Safeonweb](https://safeonweb.be/fr/apprenez-reconnaitre-les-e-mails-frauduleux), incl [phishingtest](https://safeonweb.be/fr/quiz/test-du-phishing); [Febelfin](https://www.febelfin.be/fr/article/ne-vous-faites-pas-pieger-par-la-fraude-au-ceo); [SPF Intérieur](https://www.besafe.be/fr/themes-de-securite/cybersecurite/cybercriminalite/phishing);
* Sensibiliser via le [Cyber Security KIT](https://www.cybersecuritycoalition.be/fr/resource/cyber-security-kit/) de la Cyber Security Coalition
* Authentification multifactorielle : [Cyber Security Coalition](https://www.cybersecuritycoalition.be/fr/resource/mots-passe-depasse/) & [Safeonweb](https://www.safeonweb.be/index.php/fr/lauthentification-deux-facteurs-comment-faire)
* Spoofing: [Safeonweb](https://www.safeonweb.be/fr/spoofing-lexpediteur-du-message-est-votre-adresse-e-mail)

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 Étape 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 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)

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.

### 3.1 : Identifiez vos outils et moyens

*Voir annexe VII, point 7.2 : Tableau*

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

### 3.2 : MESURES DE GESTION

**UN MAIL ENVOYE PAR VOTRE “CEO”?**

|  |  |
| --- | --- |
|  | Vérifiez l'authenticité de l'e-mail et surtout l'adresse e-mail, ne cliquez sur rien ! |
|  | Contactez votre CEO ou le service concerné par les canaux de communication habituels et demandez une confirmation. |
|  | Si le message est faux : ne répondez pas au courrier, ne le suivez pas ! Indiquez le faux expéditeur comme indésirable et bloquez-le ! |
|  | Informez le reste de l'entreprise pour que personne ne se fasse piéger |

|  |  |
| --- | --- |
|  | Signalez la tentative auprès   * + du [CERT.be](https://cert.be/fr/signaler-un-incident-0) ou via [cert@cert.be](mailto:cert@cert.be).   + la police locale, la tentative de fraude est également punissable ! |
|  | Effacez le mail. |

**TOMBE DANS LE PANNEAU ?**

|  |  |
| --- | --- |
|  | Informez les (hauts) responsables |
|  | Contactez :   * Si vous avez transféré de l'argent : contactez votre banque dès que possible ! Il est peut-être encore temps de bloquer la transaction ou de demander son annulation. * Déposer une plainte auprès de la police locale * Si vous avez souscrit une cyber-assurance et que vous avez subi un dommage : contactez votre courtier d'assurance * En cas de "violation de données" (*data breach*), n'oubliez pas de contacter [l'Autorité de protection des données](https://www.autoriteprotectiondonnees.be/professionnel/actions/fuites-de-donnees-personnelles) **endéans les 72 heures**. |
|  | Demandez au(x) responsable(s) informatique(s) (interne(s) ou externe(s)) d'effectuer une analyse antivirus, et de vérifier, avec son accord, la boîte aux lettres du CEO. |
|  | Informer le reste de l'entreprise afin que personne d'autre ne tombe dans le piège |
|  | Modifiez vos mots de passe compromis |
|  | Modifiez également toute information sensible que vous avez pu transmettre (si possible) |
|  | Envoyez le mail frauduleux au [CERT.be](https://cert.be/fr/signaler-un-incident-0) ou via [cert@cert.be](mailto:cert@cert.be). |
|  | Indiquez l'expéditeur comme indésirable et bloquez-le ! |
|  | Ne supprimez pas le courrier tant que vous n'êtes pas certain de n'avoir subi aucun dommage et que vous n'avez plus besoin de preuve. |

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 ré-adapter 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)*** |
| --- | --- | --- | --- |
| Assureur |  |  | Téléphone fixe  Bureau  1)  2)  Maison  1)  2)  Mobile  1)  2)  Email  1)  2) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| … |  |  |  |
| … |  |  |  |

### 7.2 : 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) |  |  |
| **…** |  |  |