

PHISHING

CATEGORIE : IT

 En collaboration avec :



# Phishing

**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.*

PHISHING

[I. Etape 1: Préparation (AVANT INCIDENT) 4](#_Toc57650195)

[1.1 : Placez un pilote dans l’avion 4](#_Toc57650196)

[1.2 : Connaissez vos risques 4](#_Toc57650197)

[1.3 : Mesures préventives 5](#_Toc57650198)

[II. Etape 2 : Notification et Identification 9](#_Toc57650199)

[2.1 : Notification 9](#_Toc57650200)

[2.2 : Identification 9](#_Toc57650201)

[III. Etape 3 : Activation et Traitement (INCIDENT) 10](#_Toc57650202)

[3.1 : Identifiez vos outils et moyens 10](#_Toc57650203)

[3.2 : **MESURES DE GESTION** 11](#_Toc57650205)

[IV. Etape 4 : Eradication 12](#_Toc57650207)

[V. Etape 5 : Désactivation 12](#_Toc57650208)

[VI. Etape 6 : Leçons Acquises (Post Incident Review) (APRES INCIDENT) 13](#_Toc57650209)

[6.1 : Contexte : Informations Relatives A L’incident 13](#_Toc57650210)

[6.2 : Evaluation de l’incident et leçons acquises 13](#_Toc57650211)

[VII. Annexes 17](#_Toc57650212)

[7.1 : Liste des contacts 17](#_Toc57650213)

[7.2 : Tableau 19](#_Toc57650214)

## 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.

### 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).

Selon l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), plus de 90 % des infections par des logiciels malveillants et 72 % des violations de données d'entreprise ont pour origine une attaque phishing.

Vous devez également identifier des scénarios spécifiques.

Le phishing est une forme d'escroquerie dans laquelle l'escroc (le "phisher" ou "hameçonneur") se fait passer pour une personne de confiance et tente d'amener les gens à révéler de leur plein gré des informations personnelles ou professionnelles sensibles, à cliquer sur des liens renvoyant à de faux sites web, à ouvrir des pièces jointes suspectes, ... (dans le jargon, cela s'appelle "ingénierie sociale"). La forme la plus courante de phishing se fait par e-mail, mais d'autres variantes existent également par SMS, Whats-App, appel téléphonique, médias sociaux,....

Dans l'exemple ci-dessous, vous voyez un courrier qui, à première vue, semble provenir d'une banque de confiance appelée "BANQUE X", mais en réalité, il s'agit d'un courrier de phishing. Voyez plus loin comment vous pouvez le reconnaître.

**De**: BANK X <BANK X@magenta.de>

**Date**: 11 mai 2020 à 03 :07 :30 UTC+2

**A**: Olivier.Dupont@gmail.be; Anne.Dupont@hotmail.com

**Objet**: Notification

**Répondre à:** BANK X <BANK X@magenta.de>

Cher client,

À partir du 10 mai, les premiers clients sélectionnés sont passés à la nouvelle banque en ligne. Nous avons développé et mis en œuvre les changements en collaboration avec le panel de consommateurs de la BANK X. Il faudra peut-être s'y habituer, mais avec ce nouveau visage, la banque en ligne devient plus claire et plus facile. Cela rend vos opérations bancaires quotidiennes encore plus faciles.

Remarque : vous recevrez ce bulletin d'information car vous devez encore mettre à jour votre compte pour pouvoir utiliser les services de la banque en ligne renouvelée. Après avoir rempli la demande, vous ne pourrez plus utiliser votre banque par internet pendant 24 heures.

Cliquez sur ici pour améliorer vos services et demander vos nouveaux produits.

Nous vous remercions par avance de votre coopération.

Bien à vous,

Jean Phisherman,

Service "Banque en ligne"

1.3 : Mesures préventives

#### Techniques

**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

Une attaque de phishing ne vise en général pas qu'une personne mais plusieurs : il suffit qu'une personne tombe de temps en temps dans le panneau pour que ce type d'attaque reste rentable.... Les fautes d'orthographe ou un avertissement indiquant que le message est un spam sont généralement un indice. Mais les e-mails de phishing peuvent aussi être extrêmement crédibles, avec par exemple le logo et le style de l'entreprise qu'ils copient ! Il est donc essentiel de sensibiliser et de tester tous les employés ! Si tout le monde reconnaît une attaque de phishing, le phisher n'a pratiquement aucune chance. Pour vous entrainer, un petit test de phishing est déjà disponible sur le site web [safeonweb.be.](https://www.safeonweb.be/fr/quiz/test-du-phishing)

**Caractéristiques typiques du phishing :**

* Fautes d'orthographe ou autre langue
  + **Attention : le mail de phishing peut également être correctement écrit voire reproduire assez fidèlement le logo et le style !**
* Le message se trouve dans le dossier "indésirable" ou "spam
* Le message est généralement urgent, vous devez agir rapidement, par exemple une amende qui doit être traduite ou un ami qui a besoin d'argent rapidement.
* Vous n'avez jamais entendu parler de l'expéditeur
* Vous n'attendez aucun colis du tout
* Le message est trop beau pour être vrai, par exemple vous avez gagné un smartphone coûteux sans participer à aucun concours.
* Un ami vous a marqué sur une photo sur facebook, mais vous ne vous souvenez pas avoir pris de photo ensemble et vous devez cliquer sur un lien pour vous inscrire.
* Vous n'êtes pas client à la banque qui vous a envoyé le courriel de phishing. Par ailleurs, une banque ne vous demandera jamais de fournir des informations sur votre carte de crédit, etc. par e-mail (voir le site web de [Febelfin](https://www.febelfin.be/fr/article/phishing-voici-comment-reconnaitre-un-faux-message-en-un-clin-doeil)).
* Le site web vers lequel vous êtes redirigé est suspect. Vérifiez toujours quel est le nom de la personne à contacter (qui représente le .be, .com, .eu,...) et la toute dernière barre oblique. Exemples :
  + Dans l'url https://www.**safeonweb**.be/tips, le domaine est safeonweb.
  + Dans l'url https://www.safeonweb.**tips**.be/safeonweb, "tips" est le domaine et vous serez dirigé vers un autre site web.

(Voir également la fiche fraude CEDO pour une forme plus avancée de phishing)

\*\*\*

* Il est **possible de douter** qu'un courrier soit du phishing ou un vrai courrier ! Dans ce cas :
  + Demandez un deuxième avis et/ou contactez l'institution qui vous a envoyé le courrier (par d'autres voies officielles, et non en utilisant les informations contenues dans l'email).
* **Ne partagez pas les informations internes** (sécurité, procédures, organisation interne...) avec d'autres personnes extérieures à l'entreprise (même pas sur les médias sociaux).

**VÉRIFIEZ L'ADRESSE EMAIL !**

L'adresse email vous paraît étrange, ne vous est pas familière ou vous parait avoir été créé artificiellement ? Passez le curseur de la souris sur l'adresse de l'expéditeur pour la voir en entier ! Pour distinguer le vrai du faux, voici les éléments auxquels il faut prêter attention :

* L'expéditeur semble être une entreprise de confiance, mais l'adresse électronique n'est pas professionnelle, par exemple Jean.Phisherman@noreply.com au lieu de Jean.Dupont@nomdel'entreprise.be
* L'adresse électronique semble parfaite, à part un petit détail près dans le nom de domaine, par exemple Jean.@votrebank.com au lieu de Jean@votrebanque.com ou bien par exemple la lettre "l" a été remplacée par une lettre "i" en majuscule.
* Un nom et une adresse électronique plus avancés peuvent parfaitement correspondre (dans le jargon, on dit qu'il s'agit de "spoofing"). Les réponses sont généralement redirigées vers une adresse électronique différente (l'adresse de réponse sera différente ici). En principe, un email gateway bien sécurisé arrête tous ces courriers.

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

* Mettre en place une **politique d'exécution des paiement**s.
* 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 (par exemple, le phishing) 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.
* Envisagez un point de contact central.
* **Vérifiez régulièrement vos dépenses bancaires** pour vous assurer qu'aucun mouvement suspect n'est effectué.
* Évaluez s'il pourrait être avantageux pour votre entreprise de souscrire une **cyber-assurance** qui puisse couvrir les dommages potentiels.
* 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 vos fournisseurs des canaux de communication officiels, entre eux et votre entreprise.
* 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

* [**Safeonweb**](https://safeonweb.be/fr/apprenez-reconnaitre-les-e-mails-frauduleux), incluant le [test phishing](https://www.safeonweb.be/fr/quiz/test-du-phishing)
* SPF Economie, [**qu'est ce que le phishing, comment réagir**](https://economie.fgov.be/fr/themes/line/commerce-electronique/spam/phishing)
* [**Febelfin**](https://www.febelfin.be/fr/article/phishing-voici-comment-reconnaitre-un-faux-message-en-un-clin-doeil);
* [**SPF Intérieur**](https://www.besafe.be/fr/themes-de-securite/cybersecurite/cybercriminalite/phishing)
* Sensibiliser avec le [**Cyber Security KIT**](https://www.cybersecuritycoalition.be/fr/resource/cyber-security-kit/) de la Cyber Security Coalition
* Authentification multi factorielle[:](https://www.cybersecuritycoalition.be/fr/resource/mots-passe-depasse/) **[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)
* Le [**Centre pour la Cybersécurité Belgique**](https://ccb.belgium.be/fr) (CCB)
* Pensez à vérifier le site web de votre banque : il contient certainement des informations pour lutter contre le phishing

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...

|  |  |
| --- | --- |
|  | **Pas encore cliqué ?** |
|  | Ne répondez pas au courrier, n'y donnez pas suite ! |
|  | Faites suivre le mail suspect à [suspect@safeonweb.be](mailto:suspect@safeonweb.be) |
|  | Si le mail imite votre banque : transmettez le message à votre banque via phishing@[nomdevotrebanque].be |
| ail | Indiquez l'expéditeur comme indésirable et bloquez-le |
|  | Supprimez l’email |

### 3.2 : MESURES DE GESTION

|  |  |
| --- | --- |
|  | **Déjà tombé dans le panneau ?** |
|  | Contactez le(s) responsable(s) informatique (interne ou externe) et lancez un scan antivirus.. |
|  | Modifiez votre (vos) mot(s) de passe compromis |
|  | Modifiez également toute information sensible que vous avez transmise (si possible) |
|  | **Contactez**: |
|  | * Si vous avez fourni des détails financiers : contactez votre banque dès que possible ! Avertissez Cardstop (www.cardstop.be ou 070 344 344) si nécessaire * Si de l'argent a effectivement été volé sur votre compte bancaire, déposez une plainte auprès de la police. * En cas de "violation de données" (data breach) n’oubliez pas,d’ avertir [l’Autorité de protection des données](https://www.autoriteprotectiondonnees.be/professionnel/actions/fuites-de-donnees-personnelles) endéans les 72 heures suivant la réception des données à caractère personnel * Si vous avez souscrit une cyber-assurance et que vous avez subi un dommage : contactez votre courtier d'assurance r |
|  | Transférez le mail à  suspect@safeonweb.be |
|  | Indiquez l'expéditeur comme indésirable et bloquez-le |
|  | Avisez le reste de l'entreprise que des emails d’hameçonnage (phishing) circulent |
|  | Ne supprimez pas le courrier tant que vous n'êtes pas sûr de n'avoir subi aucun dommage et que vous n'avez plus de raison de conserver 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 incident: |  |
| Gravité de incident: |  |
| Les clients ont-ils été touchés : |  |
| Gestionnaire de incident: |  |
| Description de 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) |  |  |
| **…** |  |  |