Incident   
Response Plan

Incident   
Response 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:

* Sur papier, aux endroits suivants: [Indiquer les lieux].
* 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 MATIERES

[Document : HISTORIQUE 2](#_Toc58003807)

[Historique des versions du document 2](#_Toc58003808)

[Historique des validations 2](#_Toc58003809)

[Chapitre I. Objectif du document 5](#_Toc58003810)

[Chapitre II. Liens entre les procedures 6](#_Toc58003811)

[Chapitre III. Roles 9](#_Toc58003812)

[3.1 Helpdesk 9](#_Toc58003813)

[3.2 Equipe de gestion des incidents (incident management team) 9](#_Toc58003814)

[3.3 Equipe de gestion de la continuité des activités (business continuity team) 10](#_Toc58003815)

[3.4 Equipe de gestion de la crise (crisis management team) 10](#_Toc58003816)

[Chapitre IV. INCIDENT RESPONSE PLAN 11](#_Toc58003817)

[4.1 Etape 1 Préparation 11](#_Toc58003818)

[4.2 Etape 2 Notification et identification 12](#_Toc58003819)

[4.3 Etape 3 Activation et traitement 14](#_Toc58003824)

[4.4 Etape 4 Eradication 15](#_Toc58003825)

[4.5 Etape 5 Désactivation 15](#_Toc58003826)

[4.6 Etape 6 Leçons acquises (post incident review) 16](#_Toc58003827)

[Chapitre V. Annexes 20](#_Toc58003828)

[5.1. Annexe 1. Liste des contacts 20](#_Toc58003829)

[A) Internes 20](#_Toc58003830)

[B) Externes (fournisseurs, clients,…) 22](#_Toc58003831)

[5.2 Annexe 2: documents de référence 22](#_Toc58003832)

# Chapitre I. Objectif du document

**Le principal objectif** du plan de gestion des incidents est de déterminer à l’avance comment votre entreprise traite ces incidents afin de réduire les dommages et les risques en vue de pouvoir continuer vos activités essentielles.

Ce plan de gestion des incidents établit l’organisation, les mesures et les procédures recommandées pour :

* Reconnaître un incident et y répondre ;
* Évaluer rapidement et efficacement la situation ;
* Informer les personnes et les organisations compétentes de l’incident ;
* Organiser les activités de réponse de l’entreprise, y compris l’activation d’un centre de commandement ;
* Accélérer les efforts d’intervention de l’entreprise en fonction de la gravité de l’incident ; Et
* Commencer, le cas échéant, les efforts de relance de l’entreprise au lendemain de l’incident.

Ce plan suppose que l’entreprise ait déjà réalisé un Risk Assessment et un Risk Treatment.

# Chapitre II. Liens entre les procédures

Le schéma (voir ci-dessous) indique comment la gestion des incidents s’intègre avec les autres procédures.

**1. Risk Assessment & Risk Treatment**

**2. Business Continuity Plan**

**Fournisseurs   
essentiels**

**Clients**

**B**

**A**

**B**

**C**

**D**

**E**

**E**

**F**

**H**

**G**

**G**

**I**

**H**

**J**

**A**

**3. Gestion des   
incidents  
IRP  
CMP  
DRP**

1. Pour une gestion des incidents efficace, cela suppose que l’entreprise a déjà 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. La gestion d’un incident et le plan de continuité des activités dépendront 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.**

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. Le gestionnaire de l’Incident Response Plan (IRP) avertit le gestionnaire du Crisis Management Plan (CMP) qu’un incident ayant un impact sur la continuité des activités est en cours ou est suspecté. Le gestionnaire du Crisis Management Plan maintient les gestionnaires de l’IRP informé et peut s’appuyer sur lui.
2. Le gestionnaire du Crisis Management Plan (CMP) avertit le gestionnaire du plan de continuité des activités (BCP)
3. Le gestionnaire du plan de continuité des activités (BCP) consulte et informe le gestionnaire du Crisis Management Plan (CMP)
4. Le gestionnaire du Crisis Management Plan (CMP) avertit le gestionnaire du Disaster Recovery Plan (DRP)
5. Le gestionnaire du Disaster Recovery Plan consulte et informe le gestionnaire du Management Plan Plan.
6. Les gestionnaires du Business Continuity Plan (BCP) et Disaster Recovery Plan (DRP) se tiennent mutuellement informés de l’évolution.
7. Le gestionnaire de l’Incident Response Plan (IRP) avertit le gestionnaire du Business Continuity Plan (BCP) (sans avertir le gestionnaire du Crisis Management Plan). Le gestionnaire du Business Continuity Plan peut s’appuyer sur l’Incident Response Team.

**Incident Response Plan (IRP)**

**Crisis Management Plan (CMP)**

**Disaster Recovery Plan (DRP)**

**Business Continuity Plan (BCP)**

**6**

**7**

**1**

**4**

**5**

2

**3**

Pour que le plan de continuité des activités (BCP) 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.

# Chapitre III. Rôles

Il s’agit de décrire les différents rôles et responsabilités de manière à ce que chacun connaisse le rôle qui lui est attribué.

## 3.1 Helpdesk

Le “helpdesk” ou le service en charge des incidents est chargé de mettre en place des procédures adéquates pour enregistrer les incidents, avec l'aide d'outils (softwares) appropriés.

| **Fonction** | **Rôles** |
| --- | --- |
| Gestionnaire de l’équipe Helpdesk  (Helpsdesk Manager) | * Suivi des accords de niveau de service (Service Level Agreement SLA) * Faire remonter l’information auprès du gestionnaire du plan de gestion des incidents si besoin |
| Opérateur Helpdesk  (Helpdesk Operator) | * Enregistrer les incidents et d’attribuer les priorités * Résoudre les incidents en 1ère ligne suivant les processus définis * Informer le gestionnaire de l’équipe Helpdesk |
| … |  |

## 3.2 Equipe de gestion des incidents (Incident Management Team)

L’équipe de gestion des incidents est responsable de l’exécution du plan de gestion des incidents ayant une incidence sur les processus opérationnels.

| **Fonction** | **Rôles** |
| --- | --- |
| Gestionnaire de l’équipe de gestion des incidents  Incident Response Manager) | * Élaborer et exécuter le plan de gestion des incidents pour des scenarios spécifiques. * Suivre les incidents en cours. * Avertir le gestionnaire du Crisis Management Plan et/ou le gestionnaire du plan de continuité des activités (Business Continuity Plan) |
| Membre de l’équipe de gestion des incidents  (Incident Response Team) | * Prendre l’initiative de la 2e ou de la 3e ligne de résolution des incidents mineurs ou majeurs. * Interagir avec les équipes qui aident à résoudre les incidents. |
| … |  |

## 3.3 Equipe de gestion de la continuité des activités (Business Continuity Team)

L’équipe de la continuité des activités gère l’exécution du plan de continuité des activités en cas d’incident ayant une incidence sur les processus opérationnels. Les rôles et les responsabilités de l’équipe de continuité des activités sont définis dans le plan de continuité des activités (Business Continuity Plan, voir template).

## 3.4 Equipe de gestion de la crise (Crisis Management Team)

L’Équipe de gestion des crises est responsable de la gouvernance du Plan de gestion des crises et des procédures connexes. Ils sont chargés de la coordination et de la communication en cas de catastrophe. Les rôles et responsabilités de l’équipe de gestion des crises sont définis dans le Plan de gestion des crises.

# Chapitre IV. INCIDENT RESPONSE PLAN

L’Incident Response Plan repose sur six étapes :

## 4.1 Etape 1 Préparation

Voir également Risk Assessment et Risk Treatment.

Pensez notamment à identifier les éléments suivants lors de l’élaboration de votre plan de gestion des incidents :

* Comment gérer l'incident (identifier, contenir, éliminer et récupérer les activités et les activités postérieures à l'incident)
* Surveiller, détecter, analyser et signaler les événements et incidents
* Enregistrer les incidents
* Évaluer et prendre des décisions sur les événements et les décisions
* Comment évaluer les vulnérabilités en matière de sécurité de l’information et/ou de protection de la vie privée
* Escalader les incidents (vers la Business Continuity Team ou la Crisis Management Team)
* Comment rétablir une situation normale après les incidents
* Quand communiquer, que communiquer et à qui

## 4.2 Etape 2 Notification et Identification

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.

Pensez à décrire les moyens de signaler les incidents.

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.

### 4.2.1. Faible

Lorsque l’information concernant une faiblesse ou un événement est enregistrée, l’employé désigné analyse l’information, détermine si possible la cause et, au besoin, suggère des mesures préventives et correctives.

### 4.2.2. Mineur

Lorsque des incidents mineurs sont identifiés ou signalés, l’employé désigné doit :

1. Prendre des mesures pour endiguer l’incident ;
2. Enregistrer l’incident suivant le processus applicable et évaluer la gravité en fonction des niveaux et seuils de service définis ;
3. Analyser la cause de l’incident ;
4. Prendre des mesures correctives pour éliminer la cause de l'incident (si possible, conformément au délai convenu pour la résolution);
5. Informer les intervenants touchés par l’incident ou impliqués dans l’incident de la résolution.

### 4.2.3. Majeur

Lorsque des incidents majeurs sont identifiés ou signalés, l’employé désigné doit :

1. Prendre des mesures pour endiguer l’incident ;
2. Évaluer la gravité en fonction des niveaux de service et des seuils définis. Un incident mineur peut être étendu à un incident majeur si le temps de résolution dépasse les niveaux de service convenus ou si l'impact continue d’augmenter ;
3. Informer toutes les parties prenantes responsables de l’incident survenu dans leur zone de responsabilité et indiquer le délai de résolution prévu (Voir Business Continuity Plan et Crisis Management Plan);
4. Constituer l’équipe d’intervention appropriée en cas d’incident ;
5. Surveiller l'état d'avancement de l'incident et informer de l'état d'avancement de la gestion de l’incident ;
6. Analyser la cause de l’incident ;
7. Prendre des mesures correctives pour éliminer la cause de l’incident ;
8. Informer les intervenants touchés par l’incident ou impliqués dans l’incident de la résolution.
9. Si l'incident majeur n'est pas réglé dans les délais prévus, l'incident pourrait se transformer en situation de crise selon la procédure d'escalade décrite dans le Plan de gestion des crises.

Si l’incident ne peut être résolu dans le délai prévu, le gestionnaire de l’incident response team avise immédiatement l’équipe de la continuité des activités (Business Continuity Team) et/ou l’équipe de gestion des crises (Crisis Management Team) afin d’évaluer si le plan de continuité des activités et/ou le plan de gestion des crises doivent être activés.

| **Action** | **Fonction** | **Liens vers d’autres documents**  **Nom et référence** |
| --- | --- | --- |
| Informer périodiquement le gestionnaire de crise sur la situation et le temps de reprise prévu. | Incident Manager vers le gestionnaire du Crisis Management Plan | Crisis Management Plan |
| Évaluer périodiquement le temps de retour prévu ; Si cela dépasse le Recovery Time Objective fixé (RTO), l’incident doit remonter vers l’équipe de continuité des opérations. | Incident Manager vers le gestionnaire du Business Continuity Plan | Business Continuity Plan |
| … |  |  |

### 4.2.4. Crise

En cas de crise, le plan de gestion des crises est invoqué (voir Crisis Management Plan)

**Enregistrement des incidents**

**Quelle que soit la qualification de l’incident et pendant toute la durée de celui-ci, il s’agit de conserver le journal des incidents.**

**La ou les personnes responsables de la gestion de l’incident doivent consigner toutes les mesures prises dans un registre des incidents.**

**Ce tableau ci-dessous pourrait être utilisé comme modèle pour le journal des incidents:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Date** | **Type d’incident** | **Brève description de l’incident** | **Équipe en charge** | **Description détaillée (impact, durée, activités impactées, ressources allouées,...)** | **Description des actions prises** |
| **1** |  |  |  |  |  |  |
| **2** |  |  |  |  |  |  |
| **...** |  |  |  |  |  |  |

## 4.3 Etape 3 Activation et Traitement

L’objectif principal est de réduire aussi rapidement que possible l’impact de l’incident sur la continuité des activités de l’entreprise.

Les tickets d’incident sont traités par l’incident response team en cas d’incident. Le gestionnaire de l’incident response team (leader) supervise tous les tickets. Les actions suivantes doivent être exécutées pour faire face à un incident :

| **Action** | **Fonction autorisée** | **Liens vers d’autres documents**  ***Nom et référence*** |
| --- | --- | --- |
| Effectuer une analyse rapide de la situation sur la base des informations disponibles | Opérateur Helpdesk |  |
| Déterminer les actions qui doivent être prises pour retrouver un niveau de fonctionnement minimal autorisé | Gestionnaire de l’équipe Helpdesk |  |
| Faire remonter l’incident en fonction de sa criticité | Gestionnaire de l’équipe Helpdesk vers le gestionnaire de l’Incident Response Team |  |
| Exécuter les actions à prendre | Incident response team |  |
| … |  | Voir procédures Business Continuity Plan et Crisis Management Plan |

## 4.4 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...

## 4.5 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 en accord avec le gestionnaire du Business Continuity Plan et/ou du Crisis Management 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** |
| --- | --- | --- |
| Fermer le ticket d’incident | Incident Management Team | Ticket dans le cadre de l’Incident Management |
| Désactiver l’Incident Response Plan | Incident Manager |  |
| Effectuer le Post incident Review | Incident Management Team | Post-Incident Review (document) |
| … |  |  |

## 4.6 Etape 6 Leçons acquises (Post Incident Review)

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 ;

| **Élément** | **Description** |
| --- | --- |
| **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 : |  |
| ... |  |

|  |  |
| --- | --- |
| **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 : |  |
| ... |  |

|  |  |
| --- | --- |
| **Évaluation et actions** |  |
| L'incident a-t-il été évalué correctement et correctement ?  L’information appropriée était-elle disponible pour ce faire : |  |
| Quels plans ont été activés (BCP, CMP, DRP): |  |
| Le plan de gestion des crises (CMP) 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 ? |  |
| … |  |

|  |  |
| --- | --- |
| **Activités de 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 : |  |
| … |  |

|  |  |
| --- | --- |
| **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) |  |
| ... |  |

|  |  |
| --- | --- |
| **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 : |  |
| ... |  |

|  |  |
| --- | --- |
| **Pertinence de la réponse du management** |  |
| 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, conformément au Plan de gestion des incidents :** |  |
| 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 des employés à l’incident:** |  |
| 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** |  |
| … |  |

# Chapitre V. Annexes

## 5.1. Annexe 1. Liste des contacts

### A) Internes

| **Rôle** | **Prénom et NOM** | **Fonction** | **Contacts**  **Pensez à disposer de minimum 2 contacts par rôle (1 principal et 1 en cas de maladie, congé, départ du rôle principal)** |
| --- | --- | --- | --- |
| **Leader de l’équipe de gestion de continuité ou gestionnaire du plan de continuité** |  |  | Principal  @  T  M  Autre  @  T  M |
| **Membres de l’équipe de gestion de la continuité** |  |  | Principal  @  T  M  Autre  @  T  M |
| **Service fonctionnel 1** |  | Activités essentielles (identifiez) | - Principal  @  T  M  - Autre  @  T  M |
| **Service fonctionnel 2** |  | Activités essentielles (identifiez) | - Principal  @  T  M  - Autre  @  T  M |

### B) Externes (fournisseurs, clients,…)

| **Rôle** | **Nom de la société**  **Prénom et NOM des contacts** | **Référence des contrats** | **Contacts**  **Pensez à disposer de minimum 2 contacts par rôle (1 principal et 1 en cas de maladie, congé, départ du rôle principal)** |
| --- | --- | --- | --- |
| **Fournisseur 1** |  |  | Principal  @  T  M  Autre  @  T  M |
| **Client 1** |  |  | Principal  @  T  M  Autre  @  T  M |
| **...** |  |  |  |

## 5.2 Annexe 2: Documents de référence

* Risk Assessment et Risk Treatment
* Business Continuity Plan
* Crisis Management Plan