# DOSSIER DE GESTION DES RISQUES

TRINESI

Ghilas BEKDACHE, Jonathan HAURAT, Mathieu JOILAN

# Gestion des risques

Dans un projet, la gestion des risques a pour objectif de mettre au point des plans d'actions en prévention ou en réaction à un risque. On désigne par « **risque** » tout évènement néfaste pouvant affecter une ou plusieurs dimensions du projet : les **bénéfices** attendus, son **budget**, et son **délai** de réalisation.

## I- Processus de gestion des risques

La gestion des risques passe par un processus en 6 étapes :

1. Etablissement de la liste des risques ;
2. Estimation de la gravité de chaque risque en fonction de sa probabilité d'occurrence et de son impact (selon les trois dimensions d'un projet évoquées ci-dessus) ;
3. Définition du seuil d'acceptabilité pour chaque risque ;
4. Si un risque est jugé inacceptable, analyse de ses différentes causes ;
5. Etablissement d'une stratégie de gestion pour chaque risque : Transfert, Elimination ou Réduction ;
6. Définition des actions à entreprendre.

## II- Méthodes d'identification

On dénombre deux méthodes permettant d'identifier des risques : le recours à l'expérience des acteurs, et l'approche statistique.

Dans le premier cas, des réunions de travail sont organisées en petits groupes de réflexion, où l'on cherche à liste de manière exhaustive les risques déjà rencontrés sur de projets similaires, ainsi que tout autre risque pouvant peser sur le projet actuel. La seconde méthode vient compléter la première, en présentant sous forme de statistiques les rapports d'incidents sur les projets antérieurs, ce qui peut aider à anticiper l'apparition de risques sur le projet actuel.

Pour ce projet, nous avons essentiellement fait appel à la première méthode, tout en exploitant nos expériences passées pour supporter nos estimations.

## III- Rappel du contexte

Pour rappel, le projet décrit tout au long de ce document consiste à doter le système d'information de la société IP-Sum d'une nouvelle section dans son infrastructure, avec pour objectif final que cette nouvelle section soit en mesure d'offrir un support solide et évolutif pour une solution de Cloud Computing basée sur la technologie OpenStack.

## IV- Périmètre de l'étude

Nous limitons notre étude à la seule section de l'infrastructure informatique de la société IP-Sum pour laquelle un quelconque contrat de maintenance ou de prestation de service engage notre responsabilité partielle ou totale. Cela inclut la partie physique comme la partie applicative de l'infrastructure.

A l'heure actuelle, notre périmètre d'étude se limite donc exclusivement à la nouvelle section de l'infrastructure que nous sommes chargés de configurer, livrer et installer. D'un point de vue temporel, l'étude démarre avec la conception initiale de la solution, et se poursuit jusqu'à son exploitation opérationnelle.

## V- Définition des sources de menace

Le tableau suivant liste les dix différentes catégories de risques, des exemples pour chaque catégorie, et enfin les risques retenus dans notre étude :

| Catégorie de risque | Exemple | Risques étudiés |
|---|---|---|
| Humain | Indisponibilité de ressource | • Indisponibilité de ressource ;<br>• Malveillance ;<br>• Erreur de manipulation ; |
| Méthodologique | Mauvaise planification | • Mauvaise gestion de projet ; |
| Financier | Non-obtention de financement | • Evolution des prix d'achat de matériel ; |
| Politique et stratégique | Crise économique | • Crise économique ;<br>• Acte terroriste ;<br>• Guerre ;<br>• Cyberguerre ; |
| Technique | Manque de compétences | • Manque de compétences de l'administrateur ;<br>• Panne matérielle ; |
| Juridique | Nouvelle taxe | • Apparition d'un nouvel impôt ;<br>• Modification d'une norme ; |
| Fournisseurs et partenaires | Défaillance d'un fournisseur clé | • Défaillance d'un fournisseur clé ;<br>• Bug dans le code source ; |
| Qualitatif | Non-respect du CdCF | • Non-respect du CdCF ; |
| Communication et image | Nouveau concurrent | • Apparition d'un nouveau concurrent ; |
| Naturel | Incendie | • Incendie ;<br>• Inondation ;<br>• Tremblement de terre ;<br>• Tempête solaire ;<br>• Epidémie/pandémie ; |

## VI- Glossaire de l'étude

Afin de simplifier la suite de notre étude, nous allons ici définir les principaux termes qui seront employés :

| Terme | Définition |
|---|---|
| Disponibilité | Mesure d'accessibilité d'un bien ou d'une ressource. |
| Intégrité | Mesure l'exactitude d'une donnée, afin de s'assurer qu'elle est complète et non-modifiée. |
| Confidentialité | Définit le fait qu'une donnée ne puisse être accessible que par la personne concernée. |
| Echelle de disponibilité | Mesure le délai maximum admissible pour qu'une ressource devenue inaccessible redevienne accessible. |
| Echelle d'intégrité | Permet de définir si l'altération d'une donnée est tolérée dans une certaine mesure. |
| Echelle de confidentialité | Cette échelle mesure le niveau d'accès à une ressource. |
| Echelle de gravité | Mesure le danger que représente un risque donné. |

## VII- Estimation des risques

Il convient désormais, pour chaque risque identifié précédemment, d'évaluer sa **Gravité**, notée **G**. La gravité d'un risque est le produit de son **Impact** (noté **I**, et lui-même un ensemble de trois valeurs : l'impact sur le délai (**D**), sur le coût (**C**) et sur la valeur ajoutée (**VA**)) par sa **Probabilité d'occurrence** (**P**). On a alors « GD = D * P », « GC = C * P » et « GVA = VA * P ».

Mais avant cela, il serait judicieux de présenter les différentes échelles fournissant les données de base pour l'évaluation du niveau de gravité.

### Echelle de valeurs : Disponibilité

| Niveau | Description |
|---|---|
| 48 Heures | Le bien, d'importance limitée, doit être restauré sous 48 heures en cas de panne. |
| Journée | Le bien doit être rendu disponible dans la journée. |
| Demi-journée | Le bien ne peut être inaccessible plus d'une demi-journée. |
| 1 Heure et inférieur | Toute panne sur un système si critique est intolérable, et doit être résolue dans l'heure. |

### Echelle de valeurs : Intégrité

| Niveau | Description |
|---|---|
| Négligeable | Une altération sur le bien n'a que peu d'importance. |
| Acceptable | Altération des données tolérée, à condition d'être occasionnelle, de faible importance, et détectée. |
| Intègre | Aucune altération ne sera tolérée. |

### Echelle de valeurs : Confidentialité

| Niveau | Description |
|---|---|
| Public | Le bien est accessible à tout le monde. |
| Restreint | Le bien doit seulement être accessible par un petit groupe d'individus. |
| Confidentialité | Le bien comporte des données sensibles, son accès doit être strictement règlementé et surveillé. |

### Echelle de valeurs : Probabilité d'occurrence

La probabilité d'apparition de l'événement redouté fait référence à un concept bien connu qui se mesure par un pourcentage représentant le degré de certitude selon lequel l'événement pourrait se produire. Plus ce nombre est grand, plus le risque que l'événement se produise est grand.

Dans le cadre d'un projet, on peut mesurer ce niveau de probabilité de deux manières :

- De manière mathématique en comptant le nombre de fois que l'événement s'est produit au sein des projets passés de l'organisation.
- De manière empirique en estimant un niveau de probabilité au regard de l'avis d'un groupe d'experts.

Dans notre étude, nous allons établir les valeurs de probabilité d'occurrence en nous basant sur une section temporelle **d'un an**. En effet, exprimer des pourcentages d'occurrence d'un évènement sans lui joindre une référence temporelle n'aurait aucun sens.

La suite de notre étude reposera donc sur les valeurs suivantes :

| Classe de probabilité | Intitulé de la classe | Nature des conséquences |
|---|---|---|
| P1 | Extrêmement improbable | P ≤ 1% |
| P2 | Très improbable | 1% < P ≤ 10% |
| P3 | Improbable | 10% < P ≤ 30% |
| P4 | Possible | 30% < P ≤ 70% |
| P5 | Possible à certain | 70% < P |

### Echelles de valeurs : Impact, Gravité et Niveau d'Acceptabilité

L'**Impact** d'un risque se mesure selon les trois dimensions que sont la **valeur ajoutée**, le **délai** et le **coût** du projet. Ces trois dimensions correspondent aux trois contraintes classiques auxquelles doit répondre le projet.

La **Gravité** se mesure également selon ces trois dimensions.

Afin d'éviter de nous disperser dans notre lutte contre les risques, nous allons également procéder à l'établissement du **Niveau d'Acceptabilité du Risque**, seuil en-dessous duquel le risque considéré sera jugé comme mineur, et ne sera alors pas traité dans la suite de ce document.

#### *Impact sur la Valeur Ajoutée*

| Classe d'impact | Intitulé de la classe | Nature des conséquences |
|---|---|---|
| VA1 | Mineur | Impact très faible sur la qualité des livrables du projet. Pas de réduction du périmètre fonctionnel du projet. VA ≤ 1% |
| VA2 | Significatif | Faible dégradation des performances ou de la qualité des livrables du projet. Réduction existante du périmètre fonctionnel du projet. Ne remet pas en cause la poursuite du projet. 1% < VA ≤ 5% |
| VA3 | Grave | Dégradation des performances ou de la qualité du projet. Le périmètre fonctionnel est fortement diminué. 5% < VA ≤ 7,5% |
| VA4 | Critique | Impossibilité d'atteindre une grande partie des performances attendues. Le projet pourrait ne pas être accepté par la maîtrise d'ouvrage. 7,5% < VA ≤ 10% |
| VA5 | Catastrophique | Impossibilité d'atteindre les performances attendues. Le projet ne sera pas accepté par la maîtrise d'ouvrage. 10% < VA |

#### *Gravité et Niveau d'Acceptabilité sur la Valeur Ajoutée*

En règle générale, la **Gravité** se mesure en faisant le produit de l'**Impact** par la **Probabilité**. Toutefois, un risque ayant un impact maximal ne devrait en aucun cas être négligé, y compris si sa probabilité d'occurrence reste minimale. A ce titre, nous avons établi la matrice suivante montrant le **Seuil d'Acceptabilité** en fonction des divers paramètres du risque, sans pour autant baser ce seuil sur les valeurs brutes de la **Gravité**:

| | P1 | P2 | P3 | P4 | P5 |
|---|---|---|---|---|---|
| VA1 | Niveau 1 | Niveau 1 | Niveau 1 | Niveau 2 | Niveau 2 |
| VA2 | Niveau 1 | Niveau 1 | Niveau 2 | Niveau 2 | Niveau 3 |
| VA3 | Niveau 1 | Niveau 2 | Niveau 2 | Niveau 3 | Niveau 3 |
| VA4 | Niveau 2 | Niveau 3 | Niveau 3 | Niveau 3 | Niveau 4 |
| VA5 | Niveau 3 | Niveau 3 | Niveau 3 | Niveau 4 | Niveau 4 |

Pour être plus explicite, voici un tableau décrivant les paliers relatifs aux niveaux de gravité exprimés dans le tableau ci-dessus :

| Niveau | Description |
|---|---|
| I - Négligeable | L'incident a un impact très limité, la reprise d'activité se fera facilement et rapidement. |
| II - Limitée | Quelques difficultés seront rencontrées lors du rétablissement de l'activité, la reprise pouvant prendre un peu de temps, et des données peuvent être compromises. |
| III - Importante | L'incident est grave, et demandera beaucoup de temps et de ressources afin de rétablir l'activité, avec des répercussions pouvant s'étendre sur des périodes de plusieurs semaines. |
| IV - Critique | La survie de l'entreprise est peut-être compromise. L'incident aura un tel impact qu'il faudra plusieurs mois, voire plusieurs années, pour le surmonter. |

*Impact sur le Coût*

| Classe d'impact | Intitulé de la classe | Nature des conséquences |
|---|---|---|
| C1 | Mineur | C ≤ 3% |
| C2 | Significatif | 3% < C ≤ 5% |
| C3 | Grave | 5% < C ≤ 10% |
| C4 | Critique | 10% < C ≤ 20% |
| C5 | Catastrophique | 20% < C |

*Gravité et Niveau d'Acceptabilité sur le Coût*

| | P1 | P2 | P3 | P4 | P5 |
|---|---|---|---|---|---|
| C1 | Niveau 1 | Niveau 1 | Niveau 1 | Niveau 2 | Niveau 2 |
| C2 | Niveau 1 | Niveau 1 | Niveau 2 | Niveau 2 | Niveau 3 |
| C3 | Niveau 1 | Niveau 2 | Niveau 2 | Niveau 3 | Niveau 3 |
| C4 | Niveau 2 | Niveau 3 | Niveau 3 | Niveau 3 | Niveau 4 |
| C5 | Niveau 3 | Niveau 3 | Niveau 3 | Niveau 4 | Niveau 4 |

Les paliers de valeurs du niveau de gravité sont les mêmes que ceux présentés ci-dessus.

*Impact sur le Délai*

| Classe d'impact | Intitulé de la classe | Nature des conséquences |
|---|---|---|
| D1 | Mineur | D ≤ 10% |
| D2 | Significatif | 10% < D ≤ 20% |
| D3 | Grave | 20% < D ≤ 30% |
| D4 | Critique | 30% < D ≤ 40% |
| D5 | Catastrophique | 40% < D |

*Gravité et Niveau d'Acceptabilité sur le Délai*

| | P1 | P2 | P3 | P4 | P5 |
|---|---|---|---|---|---|
| D1 | Niveau 1 | Niveau 1 | Niveau 1 | Niveau 2 | Niveau 2 |
| D2 | Niveau 1 | Niveau 1 | Niveau 2 | Niveau 2 | Niveau 3 |
| D3 | Niveau 1 | Niveau 2 | Niveau 2 | Niveau 3 | Niveau 3 |
| D4 | Niveau 2 | Niveau 3 | Niveau 3 | Niveau 3 | Niveau 4 |
| D5 | Niveau 3 | Niveau 3 | Niveau 3 | Niveau 4 | Niveau 4 |

## VIII- Evaluation des risques

Nous allons maintenant utiliser les valeurs et méthodes décrites précédemment afin d'évaluer chaque risque pesant sur notre projet, et de savoir s'ils seront retenus ou non pour la suite de l'étude :

| Tableau de synthèse : Evaluation des risques du projet | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Risques** | | | **Impact** | | | **Probabilité** | **Gravité** | | | **Commentaires** |
| **Numéro** | **Intitulé** | **Catégorie** | **VA** | **Délai** | **Coût** | | **GVA** | **GD** | **GC** | |
| 1 | Indisponibilité de ressource | Humain | 4 | 3 | 2 | 10% | 0,4 | 0,3 | 0,2 | |
| 2 | Malveillance | Humain | 2 | 5 | 4 | 50% | 1 | 2,5 | 2 | |
| 3 | Erreur de manipulation | Humain | 1 | 2 | 1 | 40% | 0,4 | 0,8 | 0,4 | |
| 4 | Mauvaise gestion de projet | Méthodologie | 5 | 5 | 5 | 5% | 0,25 | 0,25 | 0,25 | |
| 5 | Evolution des prix d'achat du matériel | Financier | 1 | 1 | 3 | 15% | 0,15 | 0,15 | 0,45 | |
| 6 | Crise économique | Politique/Stratégique | 2 | 2 | 3 | 1% | 0,02 | 0,02 | 0,03 | |
| 7 | Acte terroriste | Politique/Stratégique | 1 | 3 | 2 | < 1% | 0,01 | 0,03 | 0,02 | |
| 8 | Guerre/Cybergue rre | Politique/Stratégique | 1 | 5 | 2 | < 1% | 0,01 | 0,05 | 0,02 | Exclu de l'étude |
| 9 | Manque de compétences de l'administrateur | Technique | 4 | 4 | 2 | 10% | 0,4 | 0,4 | 0,2 | |
| 10 | Panne matérielle | Technique | 4 | 3 | 2 | 15% | 0,6 | 0,45 | 0,3 | |
| 11 | Apparition d'un nouvel impôt | Juridique | 1 | 1 | 2 | 5% | 0,05 | 0,05 | 0,1 | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 12 | Modification d'une norme | Juridique | 2 | 2 | 2 | 1% | 0,02 | 0,02 | 0,02 | |
| 13 | Défaillance d'un fournisseur clé | Fournisseurs et partenaires | 2 | 4 | 4 | 1% | 0,02 | 0,04 | 0,04 | Inclut les coupures de courant |
| 14 | Bug dans le code source | Fournisseurs et partenaires | 4 | 3 | 2 | 5% | 0,2 | 0,15 | 0,1 | |
| 15 | Non-respect du CdCF | Qualitatif | 5 | 4 | 3 | 10% | 0,5 | 0,4 | 0,3 | |
| 16 | Apparition d'un nouveau concurrent | Communication et image | 1 | 1 | 2 | 5% | 0,05 | 0,05 | 0,1 | |
| 17 | Grève/mouvement social | Communication et image | 1 | 3 | 2 | 100% | 1 | 3 | 2 | Exclu de l'étude |
| 18 | Incendie | Naturel | 1 | 5 | 5 | 5% | 0,05 | 0,25 | 0,25 | |
| 19 | Inondation | Naturel | 1 | 5 | 5 | 1% | 0,05 | 0,25 | 0,25 | |
| 20 | Tremblement de terre | Naturel | 1 | 5 | 5 | < 1% | 0,05 | 0,25 | 0,25 | Exclu de l'étude |
| 21 | Tempête solaire | Naturel | 1 | 5 | 5 | < 1% | 0,05 | 0,25 | 0,25 | Exclu de l'étude |

Seront exclus du reste de l'étude :

- Tout risque dont le niveau de gravité pour les trois dimensions est de niveau Vert ;
- Tout risque dont la probabilité d'occurrence est estimée à moins de 1%. Un commentaire « Exclu de l'étude » est présent à côté de chaque risque concerné dans le tableau précédent ;
- Tout risque contre lequel aucune mesure en notre pouvoir ne pourrait mitiger les effets. Un commentaire « Exclu de l'étude » est présent à côté de chaque risque concerné dans le tableau précédent.

## IX- Critère de gestion des risques : liste des règles qui seront utilisées

Les critères de gestion des risques retenus sont les suivants :

| Action | Critères sélectionnés pour la gestion des risques |
|---|---|
| Expression des besoins | • Les besoins de sécurité des biens essentiels sont exprimés à l'aide des échelles correspondantes, selon le critère de sécurité étudié.<br>• Les biens essentiels publics (dont le besoin en confidentialité est nul) n'engendrent pas d'événements redoutés en termes de confidentialité. |
| Estimation des événements redoutés | • Les événements redoutés sont estimés en termes de gravité et de vraisemblance à l'aide des échelles définies à cet effet. |
| Évaluation des événements redoutés | • Les événements redoutés sont classés selon leur gravité et leur vraisemblance.<br>• Les événements redoutés dont la gravité est négligeable ou la vraisemblance est invraisemblable sont jugés comme insignifiants.<br>• Ceux dont la gravité est importante ou critique et la vraisemblance est très vraisemblable ou certaine sont importants. |
| Estimation des scénarios de menaces | • Les scénarios de menaces sont estimés en termes de vraisemblance à l'aide de l'échelle définie à cet effet. |
| Évaluation des scénarios de menaces des risques | • Les scénarios de menaces sont classés par ordre décroissant de vraisemblance. |
| Estimation des risques | • La gravité d'un risque est égale à celle de l'événement redouté considéré.<br>• La vraisemblance d'un risque est égale à la vraisemblance maximale de tous les scénarios de menaces liés à l'événement redouté considéré. |
| Évaluation des risques | • Les risques doivent être triés par ordre décroissant de leur gravité et de leur vraisemblance.<br>• Les risques les plus importants sont donc les premiers de la liste triée. |
| Choix de traitement des risques | • Les risques dont les niveaux sont maximums doivent être refusés ou réduits.<br>• Les autres peuvent être refusés, réduits ou transférés. |
| Validation du traitement des risques | • Le traitement des risques ne peut être validé que s'il est démontré que les risques résiduels sont acceptables et que les mesures de sécurité destinées à traiter les risques peuvent être mises en œuvre dans un délai raisonnable. |

## X- Identification des biens

### Biens « essentiels »

Tout acteur considéré durant l'étude est lié à plusieurs processus, chacun représentant une fonction traitant des informations.

Le tableau ci-dessous regroupe tous les biens considérés comme essentiels au bon déroulement des activités :

| Services | Activités concernées |
|---|---|
| Plateforme OpenStack | • Gestion des utilisateurs<br>• Informations sensibles sur l'entreprise<br>• Point d'accès vers d'autres ressources réseau |
| Infrastructure matérielle | • Mots de passe<br>• Intégrité matérielle<br>• Performances du système |
| Infrastructure logicielle | • Données confidentielles de l'entreprise |
| Système d'exploitation | • Stabilité et intégrité du système |
| Projet | • Elaboration du projet |

### Biens « support »

Les biens support, comme leur nom l'indique, désignent en réalité les piliers sur lesquels reposent les biens essentiels.

Les biens support considérés dans notre étude sont répertoriés dans le tableau ci-dessous :

| Services | Activités concernées |
|---|---|
| Local technique | • Hébergement<br>• Accès réseaux<br>• Sécurités physiques (sur accès, et mesures anti-catastrophes) |
| Stockage RAID | • Accessibilité hautes performances des ressources, première couche de redondance |
| Systèmes de sauvegarde/redondance/haute disponibilité | • Sécurité du système en cas de panne ou de pic d'activité |
| Ressources humaines | • Compétences techniques et fonctionnelles |

### Table de correspondance entre les biens essentiels et les biens supports

Le tableau ci-dessous permet de faire ressortir les liens éventuels entre des biens essentiels (**BE**) et des biens support (**BS**), et ce, afin de mieux cerner le fonctionnement global du système, ainsi que les probables répercutions d'un incident affectant un sous-système :

| BE / BS | Gestion utilisateurs | Informations sensibles | Point d'accès vers d'autres ressources réseau | Mots de passe | Intégrité matérielle | Performances du système | Données confidentielles de l'entreprise | Stabilité et intégrité du système | Projet |
|---|---|---|---|---|---|---|---|---|---|
| Hébergement | √ | √ | √ | √ | √ | √ | √ | √ | |
| Accès réseaux | | √ | √ | | | √ | | | |
| Sécurités physiques | √ | √ | √ | √ | √ | | √ | √ | |
| Stockage | | √ | | | √ | √ | | √ | |
| Haute disponibilité | | √ | | | √ | √ | | √ | |
| Compétences | | | | | | | | | √ |

## IX - Etude des évènements redoutés

Il convient maintenant d'établir un tableau associant, à chaque Evènement Redouté (ou **ER**), le bien essentiel impacté, le besoin de sécurité affecté, une brève description de l'impact plausible, les principales sources connues pour l'ER étudié, et une estimation de la gravité.

| N° | Evènement redouté | Besoin de sécurité | Impact | Sources connues | Gravité |
|---|---|---|---|---|---|
| Infrastructure physique | | | | | |
| ER1 | Panne matérielle | Intégrité | • Perte d'accès<br>• Dégradation de performances<br>• Perte de données | • Défaillance matérielle<br>• Environnement<br>• Malveillance | **Critique** |
| ER2 | Acte de malveillance | Restriction d'accès | • Idem qu'ER1<br>• Vol de données | • Piratage<br>• Employé mécontent | **Critique** |
| ER3 | Arrêt imprévu | Disponibilité | • Perte de fonctionnalités<br>• Indisponibilité des ressources | • Coupure de courant<br>• Sinistre<br>• Inattention<br>• Malveillance | Importante |
| • Plateforme OpenStack | | | | | |
| ER4 | Arrêt de service | Disponibilité | • Perte de fonctionnalités<br>• Indisponibilité des ressources | • Incident logiciel<br>• Bug dans le code source<br>• Incident matériel<br>• Inattention<br>• Malveillance | Importante |
| ER5 | Défaillance d'un hôte | Disponibilité<br>Intégrité | • Indisponibilité des ressources<br>• Perte de données | • Incident logiciel<br>• Incident matériel<br>• Inattention | Limitée |
| ER6 | Non-respect du CdCF | Disponibilité | • Manque de fonctionnalités<br>• Retards | • Mauvaise gestion de projet<br>• Manque de compétences | **Critique** |
| • Infrastructure logicielle | | | | | |
| ER7 | Arrêt d'une dépendance | Disponibilité | • Perte d'accès<br>• Dégradation de performances<br>• Perte de fonctionnalités | • Incident logiciel<br>• Bug dans le code source<br>• Incident matériel<br>• Inattention<br>• Echec de mise à jour | Limitée |
| • Système d'exploitation | | | | | |
| ER8 | Défaillance d'un service annexe | Intégrité<br>Disponibilité | • Perte d'accès<br>• Dégradation de performances<br>• Perte de fonctionnalités | • Incident logiciel<br>• Bug dans le code source<br>• Incident matériel<br>• Inattention<br>• Echec de mise à jour<br>• Malveillance | Limitée |
| ER9 | Défaillance d'un service critique | Intégrité<br>Disponibilité | • Idem<br>• Perte de données | • Idem | **Critique** |

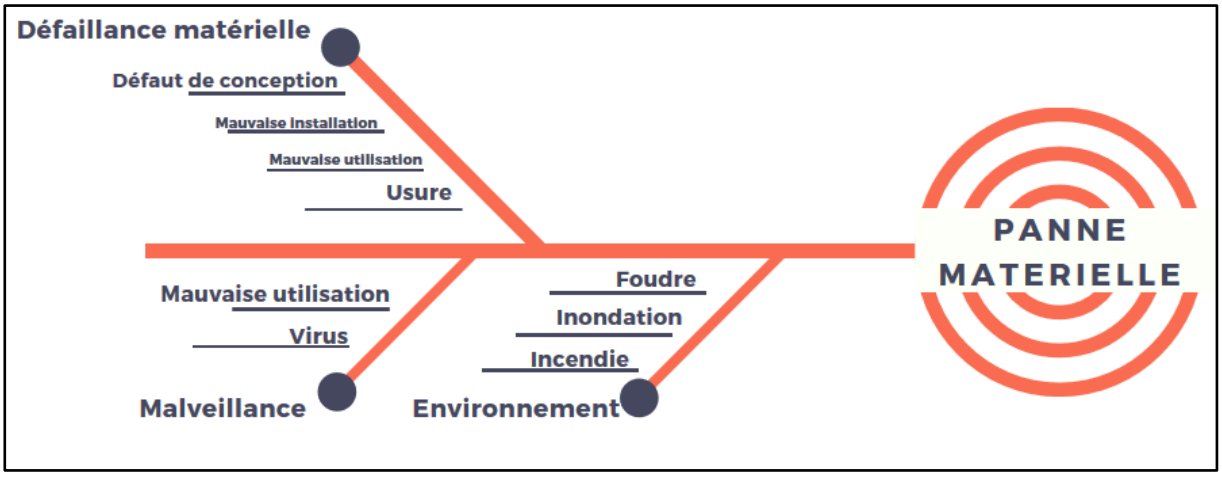
Nous pouvons également présenter ces risques sous la forme d'un tableau classant les évènements redoutés par gravité décroissante :

| Gravité | ER |
|---|---|
| Critique | Défaillance d'un service critique<br>Acte de malveillance<br>Panne matérielle<br>Non-Respect du CdCF |
| Importante | Arrêt imprévu du matériel<br>Arrêt de service |
| Limitée | Défaillance d'un hôte<br>Arrêt d'une dépendance<br>Défaillance d'un service annexe |
| Négligeable | |

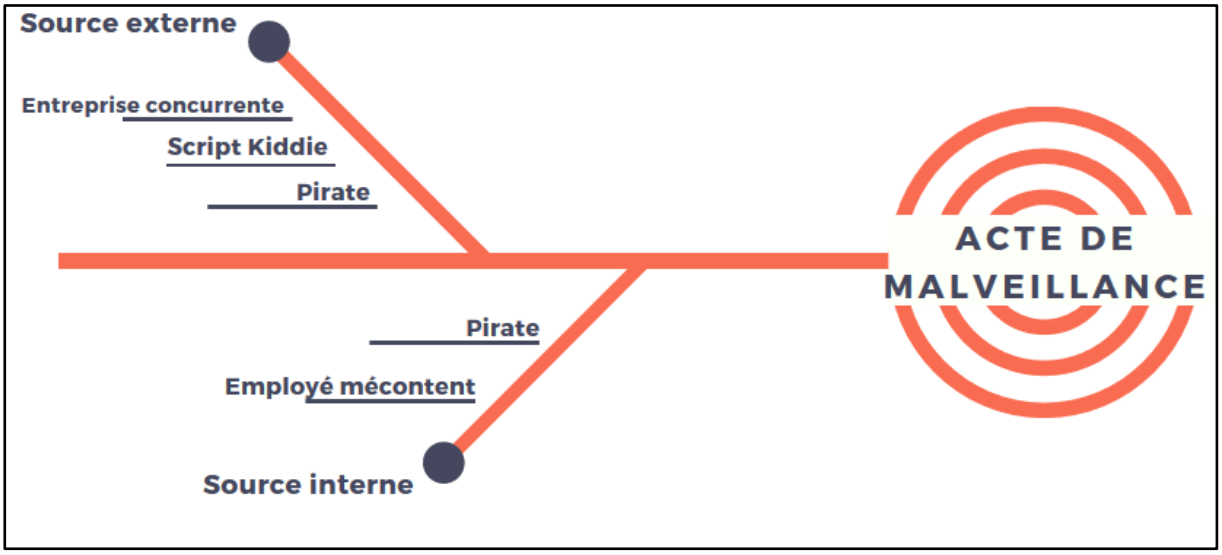
### Ishikawa

Il est aussi possible de dresser un diagramme d'Ishikawa pour chacun des évènements redoutés mentionnés au tableau de la page précédente. Nous allons toutefois nous limiter aux risques dont la gravité est Importante ou Critique.

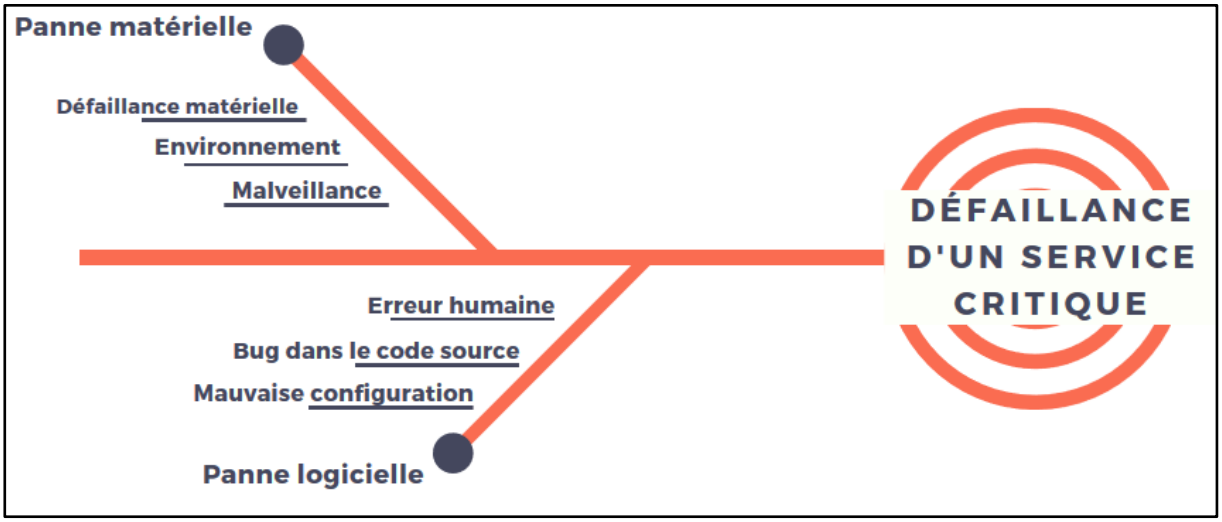
#### *Panne matérielle*



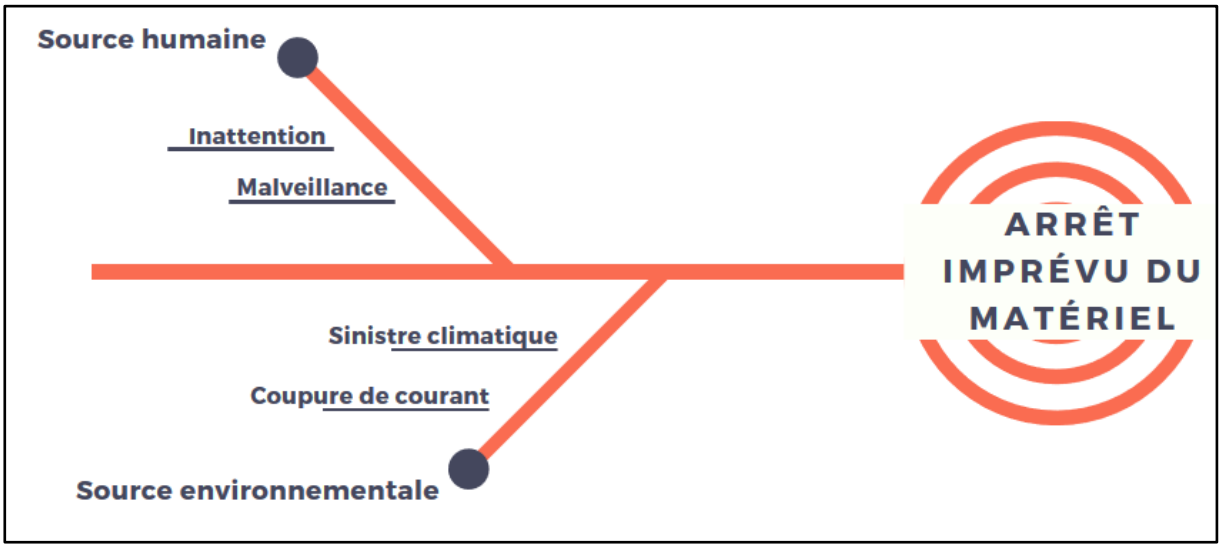
*Acte de malveillance*



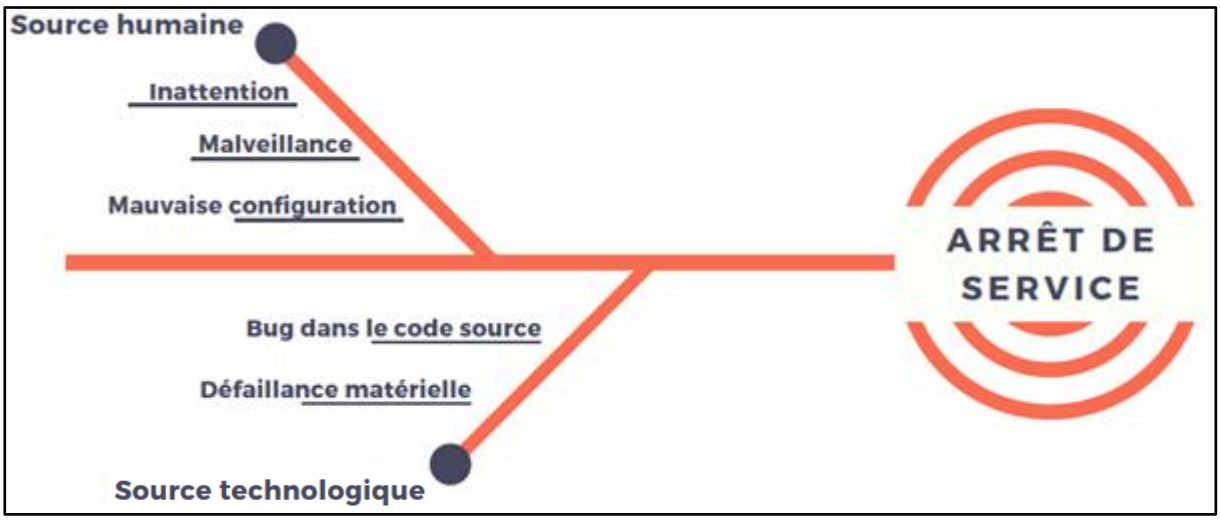

*Défaillance d'un service critique*



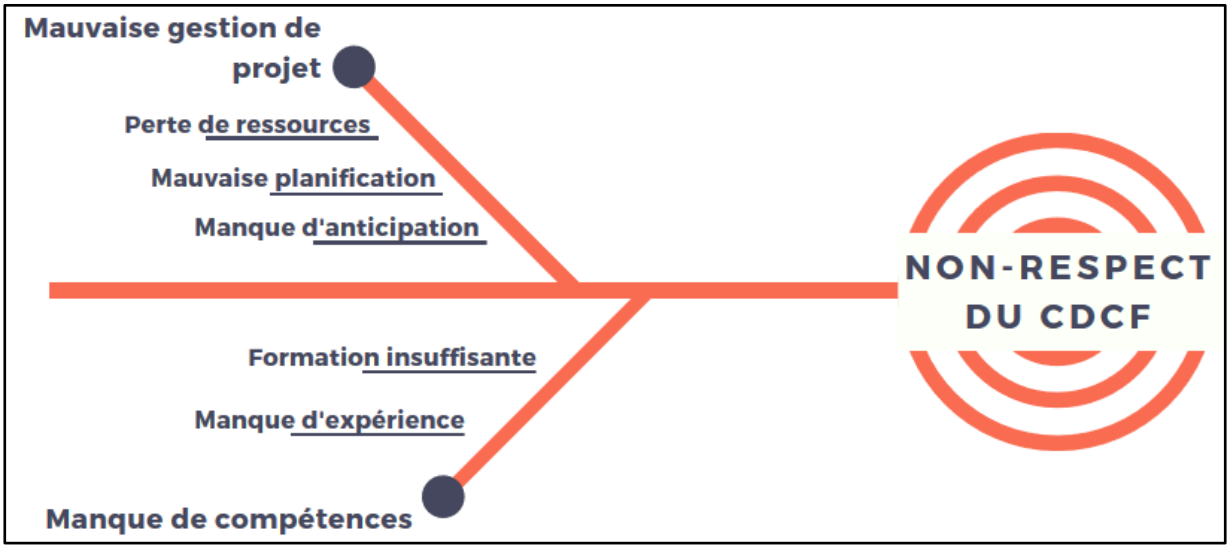

*Arrêt imprévu du matériel*



*Arrêt de service*




*Non-Respect du CdCF*



## X - Etude des scénarios de menaces

Dans le cadre d'une étude EBIOS, un scénario de menace vise à indiquer de quelle manière une menace peut compromettre le bon déroulement des opérations du système, les sources potentielles, ainsi que la vraisemblance d'occurrence d'un tel scénario.

Nous allons également établir des scénarios de menace propres au projet.

| N° | Scénario | Sources connues | Vraisemblance |
|---|---|---|---|
| Infrastructure | | | |
| ScM1 | Menace (infrastructure) ayant un impact sur la disponibilité | 1. Opération de maintenance<br>2. Coupure de courant<br>3. Panne matérielle | Importante |
| | | 4. Acte de malveillance<br>5. Erreur d'inattention<br>6. Incendie (ou autre catastrophe) | Limitée |
| ScM2 | Menace (infrastructure) ayant un impact sur l'intégrité | 1. Défaillance matérielle<br>2. Acte de malveillance<br>3. Erreur d'inattention | Limitée |
| ScM3 | Menace (infrastructure) ayant un impact sur la confidentialité | 1. Acte de malveillance | Limitée |
| | | 2. Inattention, mauvaise configuration | Négligeable |
| Projet | | | |
| ScM4 | Menace ayant un impact sur le déroulement du projet | 1. Perte d'une ressource | Négligeable |
| | | 2. Requalification des besoins par le client | Limitée |
| Autres | | | |
| ScM5 | Autre menace ayant un impact sur la disponibilité | 1. Incident chez fournisseur d'accès internet | Limitée |

Au même titre que dans le cas des évènements redoutés, nous pouvons ici classer les scénarios de menace par ordre décroissant de vraisemblance :

| Vraisemblance | Scénario de menace |
|---|---|
| Critique | |
| Importante | Menace (infrastructure) ayant un impact sur la disponibilité |
| Limitée | Menace (infrastructure) ayant un impact sur la disponibilité<br>Menace (infrastructure) ayant un impact sur l'intégrité<br>Menace (infrastructure) ayant un impact sur la confidentialité<br>Menace ayant un impact sur le déroulement du projet<br>Autre menace ayant un impact sur la disponibilité |
| Négligeable | Menace (infrastructure) ayant un impact sur la confidentialité<br>Menace ayant un impact sur le déroulement du projet |

# XI - Analyse des risques

## XI.1 - Humains

### *XI.1.1 - Malveillance*

**Description** : Exploitation d'une faille par une personne non-autorisée.

| Niveau de risque | | | | |
|---|---|---|---|---|
| Gravité | Négligeable | Limitée | Importante | **Critique** |
| Vraisemblance | Négligeable | ~~Limitée~~ | Importante | ~~Critique~~ |

**Légende** : La gravité d'un tel incident peut varier de « Négligeable » à « Critique » suivant la nature de la faille exploitée. La vraisemblance, quant à elle, est assez élevée.

**Impact** : Vol, modification et/ou suppression de données.

**Scénarios de menaces** :

| Scénario de menace | Sources potentielles | Vraisemblance |
|---|---|---|
| Menace venant de l'extérieur du réseau de l'entreprise | Attaquant externe exploitant une faille ou une série de failles | Importante |
| Menace venant de l'intérieur du réseau de l'entreprise | Employé cherchant à nuire à l'entreprise | Négligeable |

**Mesures préventives et correctives** :

| Mesures de sécurité | Biens supports | Prévention | Protection | Récupération |
|---|---|---|---|---|
| Fermeture de ports de communications non-utilisés | • Accès réseaux<br>• Hébergement | √ | √ | |
| Modification des ports par défaut | • Accès réseaux<br>• Hébergement | √ | | |
| Implémentation de systèmes anti-intrusion | • Accès réseaux<br>• Hébergement | √ | √ | |
| Sauvegarde des données | • Hébergement | | | √ |

### *XI.1.2 - Indisponibilité de ressources*

**Description** : Perte imprévue d'une ressource clé de l'équipe de réalisation du projet.

| Niveau de risque | | | | |
|---|---|---|---|---|
| Gravité | Négligeable | Limitée | Importante | **Critique** |
| Vraisemblance | Négligeable | ~~Limitée~~ | ~~Importante~~ | ~~Critique~~ |

**Légende** : Sans une anticipation adéquate, la perte d'une ressource peut s'avérer catastrophique pour l'avenir d'un projet. Heureusement, la probabilité d'occurrence d'un tel évènement reste très faible.

**Impact** : Réduction du périmètre du projet, allongement des délais, dépassement de budget.

**Scénarios de menaces** :

| Scénario de menace | Sources potentielles | Vraisemblance |
|---|---|---|
| Perte d'une ressource | • Blessure grave<br>• Décès | Négligeable |

**Mesures préventives et correctives** :

| Mesures de sécurité | Biens | Prévention | Protection | Récupération |
|---|---|---|---|---|
| Harmonisation des compétences entre les membres de l'équipe | • Compétences | | √ | |
| Insertion d'une « marge d'erreur » dans la prévision calendaire | • Compétences | √ | | |

### *XI.1.3 - Erreur de manipulation*

**Description** : Erreur humaine lors d'une phase d'installation, de configuration, de modification ou d'exploitation de la solution.

| Niveau de risque | | | | |
|---|---|---|---|---|
| Gravité | Négligeable | Limitée | Importante | ~~Critique~~ |
| Vraisemblance | ~~Négligeable~~ | Limitée | ~~Importante~~ | ~~Critique~~ |

**Légende** : Une erreur humaine peut avoir des conséquences et des répercussions potentiellement importantes. Toutefois, le risque de voir un tel évènement survenir lors de la conception et l'implémentation de la solution est faible.

**Impact** : Dégradation de services ou de matériels, allongement des délais, dépassement de budget.

**Scénarios de menaces** :

| Scénario de menace | Sources potentielles | Vraisemblance |
|---|---|---|
| Mauvaise configuration du système | • Erreur d'inattention<br>• Manque de compétences | Limitée |

**Mesures préventives et correctives** :

| Mesures de sécurité | Biens | Prévention | Protection | Récupération |
|---|---|---|---|---|
| Partage de connaissances entre les membres du groupe de projet | • Compétences | √ | | |
| Vérification par un tiers lors des phases critiques | • Compétences | | √ | |

## XI.2 - Méthodologie

### *XI.2.1 - Mauvaise gestion de projet*

**Description** : Incapacité du chef de projet d'avoir une vision claire du projet, et d'assigner efficacement les ressources sur les tâches.

| Niveau de risque | | | | |
|---|---|---|---|---|
| Gravité | ~~Négligeable~~ | ~~Limitée~~ | Importante | **Critique** |
| Vraisemblance | Négligeable | ~~Limitée~~ | ~~Importante~~ | ~~Critique~~ |

**Légende** : Ce genre d'incident n'a que peu de chances de se produire, mais lorsque cela arrive, les conséquences sont presque toujours critiques.

**Impact** : Vol/destruction de données.

**Scénarios de menaces** :

| Scénario de menace | Sources potentielles | Vraisemblance |
|---|---|---|
| Non-respect du CdCF | • Manque de vision du chef de projet<br>• Mauvaise allocation de ressources | Négligeable |
| Dépassement de budget et/ou de délais | Idem | Négligeable |

**Mesures préventives et correctives** :

| Mesures de sécurité | Biens | Prévention | Protection | Récupération |
|---|---|---|---|---|
| Adoption d'une méthode Agile | • Compétences | √ | √ | |

## XI.3 - Financier

### *XI.3.1 - Evolution des prix d'achat du matériel*

**Description** : Augmentation des prix d'achat du matériel.

| Niveau de risque | | | | |
|---|---|---|---|---|
| Gravité | Négligeable | Limitée | ~~Importante~~ | ~~Critique~~ |
| Vraisemblance | ~~Négligeable~~ | Limitée | ~~Importante~~ | ~~Critique~~ |

**Légende** : Suivant le contexte économique global, une évolution des tarifs auprès de nos fournisseurs est bien sûr à envisager. Toutefois, il est raisonnable de penser que, si cela devait se produire, l'augmentation resterait modeste sur une courte période de temps.

**Impact** : Dépassement de budget.

**Scénarios de menaces** :

| Scénario de menace | Sources potentielles | Vraisemblance |
|---|---|---|
| Augmentation des tarifs pour du matériel informatique | • Fournisseur<br>• Crise économique | Limitée |

**Mesures préventives et correctives** :

| Mesures de sécurité | Biens | Prévention | Protection | Récupération |
|---|---|---|---|---|
| Limiter au mieux le délai entre la validation client et la commande du matériel | | √ | √ | |
| Si augmentation mineure, réduction de notre marge pour ne pas impacter le client | | | | √ |
| Si augmentation importante, actualisation du budget auprès du client | | | | √ |

### *XI.4 - Technique*

#### *XI.4.1 - Manque de compétences de l'administrateur*

**Description** : L'administrateur de la solution ne dispose pas des compétences adéquates.

| Niveau de risque | | | | |
|---|---|---|---|---|
| Gravité | ~~Négligeable~~ | Limitée | Importante | ~~Critique~~ |
| Vraisemblance | ~~Négligeable~~ | Limitée | ~~Importante~~ | ~~Critique~~ |

**Légende** : OpenStack étant une solution complexe d'utilisation et à administrer, le risque de voir un administrateur utiliser la solution sans avoir reçu la formation adéquate n'est pas négligeable. Les conséquences peuvent toutefois être graves.

**Impact** : Perte de fonctionnalités, baisse de performances, dégradation des services.

**Scénarios de menaces** :

| Scénario de menace | Sources potentielles | Vraisemblance |
|---|---|---|
| Perte d'une fonctionnalité | Administrateur | Limitée |
| Arrêt d'un service | Administrateur | Limitée |

**Mesures préventives et correctives** :

| Mesures de sécurité | Biens | Prévention | Protection | Récupération |
|---|---|---|---|---|
| Formation technique aux administrateurs | • Compétences | √ | √ | |

### *XI.4.1 - Panne matérielle*

**Description** : Défaillance d'un composant ou d'un ensemble de composants.

| Niveau de risque | | | | |
|---|---|---|---|---|
| Gravité | Négligeable | Limitée | Importante | **Critique** |
| Vraisemblance | ~~Négligeable~~ | Limitée | ~~Importante~~ | ~~Critique~~ |

**Légende** : La perte d'un composant est inévitable (usure normale des pièces), mais si le risque n'est pas correctement évalué en amont, ses conséquences peuvent être très graves.

**Impact** : Perte de fonctionnalités, baisse de performances, dégradation des services, perte de données.

**Scénarios de menaces** :

| Scénario de menace | Sources potentielles | Vraisemblance |
|---|---|---|
| Dégradation de performances | Perte d'un composant | Limitée |
| Arrêt de service | Perte d'un ensemble de composants | Limitée |
| Perte de données | Perte d'un composant ou d'un ensemble de composants | Limitée |

**Mesures préventives et correctives** :

| Mesures de sécurité | Biens | Prévention | Protection | Récupération |
|---|---|---|---|---|
| Redondance matérielle | • Hébergement<br>• Accès réseaux | √ | √ | |
| Matériel de rechange | • Hébergement<br>• Accès réseaux | | | √ |
| Sauvegarde | • Hébergement | | | √ |

## XI.5 - Fournisseurs et partenaires

### *XI.5.1 - Défaillance d'un fournisseur clé*

**Description** : Défaillance d'un fournisseur de services majeurs.

| Niveau de risque | | | | |
|---|---|---|---|---|
| Gravité | ~~Négligeable~~ | Limitée | Importante | **Critique** |
| Vraisemblance | Négligeable | ~~Limitée~~ | ~~Importante~~ | ~~Critique~~ |

**Légende** : La perte d'un fournisseur majeur peut être critique, notamment s'il s'agit d'u fournisseur d'électricité ou d'un service majeur.

**Impact** : Perte de fonctionnalités, arrêt total d'exploitation.

**Scénarios de menaces** :

| Scénario de menace | Sources potentielles | Vraisemblance |
|---|---|---|
| Perte de fonctionnalités | Perte d'un fournisseur de services numériques | Négligeable |
| Arrêt total d'exploitation | Perte d'un fournisseur de services communs | Négligeable |

**Mesures préventives et correctives** :

| Mesures de sécurité | Biens | Prévention | Protection | Récupération |
|---|---|---|---|---|
| Si possible, faire appel à des concurrents | • Hébergement<br>• Accès réseaux | √ | √ | √ |

### *XI.5.2 - Bug dans le code source*

**Description** : Erreur de programmation non-repérée lors de la publication d'une source logicielle.

| Niveau de risque | | | | |
|---|---|---|---|---|
| Gravité | Négligeable | Limitée | Importante | ~~Critique~~ |
| Vraisemblance | ~~Négligeable~~ | Limitée | Importante | ~~Critique~~ |

**Légende** : Il arrive bien souvent qu'une nouvelle version d'un logiciel apporte son lot de nouveaux bugs, parfois avec des conséquences importantes.

**Impact** : Apparition de nouvelles failles de sécurité, perte de fonctionnalités.

**Scénarios de menaces** :

| Scénario de menace | Sources potentielles | Vraisemblance |
|---|---|---|
| Perte de fonctionnalités | Erreur dans le code source | Limitée |
| Apparition de nouvelles failles | Idem | Importante |

**Mesures préventives et correctives** :

Utiliser la version N-1 du logiciel permet de bénéficier d'une version stable, mais en contrepartie, cette version N-1 risque de présenter des failles corrigées dans la version N.

| Mesures de sécurité | Biens | Prévention | Protection | Récupération |
|---|---|---|---|---|
| Utiliser la version N-1 du logiciel | • Infrastructure logicielle | √ | | |

## XI.6 - Qualitatif

### *XI.6.1 - Non-respect du CdCF*

**Description** : Le produit final ne réponds pas aux attentes exprimées par le client.

| Niveau de risque | | | | |
|---|---|---|---|---|
| Gravité | ~~Négligeable~~ | ~~Limitée~~ | ~~Importante~~ | **Critique** |
| Vraisemblance | ~~Négligeable~~ | Limitée | ~~Importante~~ | ~~Critique~~ |

**Légende** : Bien que peu probable, l'impact que représente un tel risque est catastrophique, le client risquant de ne pas accepter le produit.

**Impact** : Refus du produit par le client.

**Scénarios de menaces** :

| Scénario de menace | Sources potentielles | Vraisemblance |
|---|---|---|
| Le produit n'offre pas les fonctionnalités attendues par le client | Mauvaise gestion de projet | Limitée |

**Mesures préventives et correctives** :

| Mesures de sécurité | Biens | Prévention | Protection | Récupération |
|---|---|---|---|---|
| Faire régulièrement des réunions d'information auprès du client | • Projet | √ | √ | |
| Au besoin, réajuster le déroulé futur du projet | • Projet | | | √ |

## XI.7 - Naturel

### *XI.7.1 - Incendie*

**Description** : Incendie des locaux.

| Niveau de risque | | | | |
|---|---|---|---|---|
| Gravité | ~~Négligeable~~ | ~~Limitée~~ | Importante | **Critique** |
| Vraisemblance | ~~Négligeable~~ | Limitée | ~~Importante~~ | ~~Critique~~ |

**Légende** : Compte tenu de la chaleur dégagée par les serveurs et autres composants actifs, ainsi que de la présence de forts courants électriques, le risque de voir un incendie se déclencher dans une salle serveurs ne peut être négligé, d'autant que ses conséquences sont obligatoirement très graves.

**Impact** : Perte de données, arrêt de production.

**Scénarios de menaces** :

| Scénario de menace | Sources potentielles | Vraisemblance |
|---|---|---|
| Perte de données | Destruction de matériel | Limitée |

**Mesures préventives et correctives** :

| Mesures de sécurité | Biens | Prévention | Protection | Récupération |
|---|---|---|---|---|
| Détecteurs d'incendie | • Hébergement | √ | | |
| Systèmes d'extinction d'incendie | • Hébergement | | √ | |
| Sauvegarde des données sur site externe | • Stockage | | | √ |
| Mise en place d'un site de secours | • Stockage<br>• Hébergement<br>• Accès réseaux | | | √ |

### *XI.7.2 - Inondation*

**Description** : Inondation des locaux.

| Niveau de risque | | | | |
|---|---|---|---|---|
| Gravité | ~~Négligeable~~ | ~~Limitée~~ | ~~Importante~~ | **Critique** |
| Vraisemblance | Négligeable | ~~Limitée~~ | ~~Importante~~ | ~~Critique~~ |

**Légende** : Suivant l'emplacement des locaux, ainsi que la disposition des conduites d'eau, il est possible que la salle serveurs subisse un dégât des eaux.

**Impact** : Perte de données, arrêt de production.

**Scénarios de menaces** :

| Scénario de menace | Sources potentielles | Vraisemblance |
|---|---|---|
| Perte de données | Destruction de matériel | Négligeable |

**Mesures préventives et correctives** :

| Mesures de sécurité | Biens | Prévention | Protection | Récupération |
|---|---|---|---|---|
| Sauvegarde des données sur site externe | • Stockage | | | √ |
| Mise en place d'un site de secours | • Stockage<br>• Hébergement<br>• Accès réseaux | | | √ |

## Fiches récapitulatives des risques

| **Projet** : CLOUDIFY | | **Risque** : Malveillance | | |
|---|---|---|---|---|
| Date d'identification : 22/05/2019<br>Responsable du risque :<br>Jonathan HAURAT | | **N°** : 1 | Famille de risques : Humain | |
| Description du risque :<br>Exploitation d'une faille ou d'une série de failles par une personne non-autorisée. | | | | |
| Etat du risque :<br>LATENT | Probabilité estimée : 50% | Impact coût :<br>NIV. IV | Impact délai :<br>NIV. V | Impact VA :<br>NIV. II |
| Actions de surveillance du risque :<br>• Implémentation de systèmes anti-intrusion | | | | |
| Actions préventives :<br>• Fermeture de ports de communication non-utilisés<br>• Modification des ports par défaut | | | | |
| Actions correctives :<br>• Sauvegarder les données | | | | |

| **Projet :** CLOUDIFY | | **Risque :** Indisponibilité de ressource humaine | | |
|---|---|---|---|---|
| Date d'identification : 22/05/2019<br>Responsable du risque :<br>Jonathan HAURAT | | **N°** : 2 | Famille de risques : Humain | |
| Description du risque :<br>A ce jour, nous comptons 4 personnes dans l'entreprise. L'indisponibilité prolongée de chacune d'entre elles est à prendre en compte afin d'amoindrir les risques de productivité et parer le blocage totale d'activité. | | | | |
| Etat du risque :<br>LATENT | Probabilité estimée : 10% | Impact coût :<br>NIV. II | Impact délai :<br>NIV.III | Impact VA : NIV. IV |
| Actions de surveillance du risque :<br>• Se montrer à l'écoute de chacun | | | | |
| Acton préventive :<br>• Entretien annuelle | | | | |
| Actions correctives :<br>• Faire en sorte que chaque employé soit polyvalent<br>• Le nombre d'employés actuel a la capacité à absorber la charge de travail en cas de la perte de 25% de ressource humaine (1 personne). | | | | |

| **Projet :** CLOUDIFY | | **Risque :** Erreur de manipulation | | |
|---|---|---|---|---|
| Date d'identification : 22/05/2019<br>Responsable du risque :<br>Jonathan HAURAT | | **N°** : 3 | Famille de risques : Humaine | |
| Description du risque :<br>L'erreur de manipulation peut arriver par une faute de frappe, et provoquer des erreurs de configuration pouvant empêcher le bon fonctionnement du produit | | | | |
| Etat du risque :<br>LATENT | Probabilité estimée : 50% | Impact coût :<br>NIV. I | Impact délai :<br>NIV. II | Impact VA :<br>NIV. I |
| Actions de surveillance du risque :<br>• Tester le produit | | | | |
| Actions préventive :<br>• Tester le produit | | | | |
| Actions correctives :<br>• Script d'installation automatique | | | | |

| **Projet :** CLOUDIFY | | **Risque :** Mauvaise gestion de projet | | |
|---|---|---|---|---|
| Date d'identification : 22/05/2019<br>Responsable du risque :<br>Jonathan HAURAT | | **N°** : 4 | Famille de risques : Méthodologie | |
| Description du risque :<br>Une mauvaise gestion de projet peut mener à des retards, des non faits, finalement à un projet mal mené et la perte d'un client. | | | | |
| Etat du risque :<br>LATENT | Probabilité estimée : 5% | Impact coût :<br>NIV. V | Impact délai :<br>NIV. V | Impact VA :<br>NIV. V |
| Actions de surveillance du risque :<br>• Gantt | | | | |
| Actions préventives :<br>• Outils de gestion de projet : Gestanesi, Méthode Agile Scrum, communication forte en interne, Gantt. | | | | |
| Actions correctives : | | | | |

| **Projet :** CLOUDIFY | | **Risque :** Evolution des prix d'achat du matériel | | |
|---|---|---|---|---|
| Date d'identification : 22/05/2019<br>Responsable du risque :<br>Jonathan HAURAT | | **N°** : 5 | Famille de risques : Financier | |
| Description du risque :<br>Entre le moment où le devis est validé par le client, et celui où le matériel est commandé, le prix repéré peut changer. | | | | |
| Etat du risque :<br>LATENT | Probabilité estimée : 15% | Impact coût :<br>NIV. III | Impact délai :<br>NIV. I | Impact VA :<br>NIV. I |
| Actions de surveillance du risque :<br>• Veille technologique et économique des fournisseurs | | | | |
| Actions préventives : | | | | |
| Actions correctives : | | | | |

| **Projet :** CLOUDIFY | | **Risque :** Manque de compétences de l'administrateur | | |
|---|---|---|---|---|
| Date d'identification : 22/05/2019<br>Responsable du risque :<br>Jonathan HAURAT | | **N°** : 6 | Famille de risques : Technique | |
| Description du risque :<br>Le manque de compétences peut provoquer des pannes, des mauvaises manipulations, une perte client. Ce problème peut survenir à cause de la complexité de la technologie | | | | |
| Etat du risque :<br>LATENT | Probabilité estimée : 10% | Impact coût :<br>NIV. II | Impact délai :<br>NIV. IV | Impact VA :<br>NIV. IV |
| Actions de surveillance du risque : | | | | |
| Actions préventive :<br>• Lors du recrutement, s'assurer du niveau de compétences du collaborateur<br>• Formation continue des employés<br>• Rédaction de documentations administrateurs/utilisateur | | | | |
| Actions correctives : | | | | |

| **Projet :** CLOUDIFY | | **Risque :** Panne matérielle | | |
|---|---|---|---|---|
| Date d'identification : 22/05/2019<br>Responsable du risque :<br>Jonathan HAURAT | | **N°** : 7 | Famille de risques : Technique | |
| Descriptif du risque :<br>Avec l'usure normale, tout matériel peut tomber en panne. | | | | |
| Etat du risque :<br>LATENT | Probabilité estimée : 15% | Impact coût :<br>NIV. II | Impact délai :<br>NIV. III | Impact VA :<br>NIV. IV |
| Actions de surveillance du risque :<br>• Monitoring automatique sur les équipements compatibles<br>• Tests logiciels périodiques | | | | |
| Actions préventive :<br>• Conseil de prise de garanties à l'achat<br>• Mise en place de haute disponibilité | | | | |
| Actions correctives :<br>• Remplacement des pièces défectueuses par du matériel de rechange | | | | |

| **Projet :** CLOUDIFY | | **Risque :** Défaillance d'un fournisseur clé | | |
|---|---|---|---|---|
| Date d'identification : 22/05/2019<br>Responsable du risque :<br>Jonathan HAURAT | | **N°** : 8 | **Famille de risques :** Fournisseurs & partenaires | |
| Description du risque :<br>Si un fournisseur ne peut plus nous livrer nos produits, que ce soit pour des raisons politiques, de priorité, de coupure de courant ou de faillite, cela peut menacer notre productivité, ainsi que la satisfaction du client. | | | | |
| Etat du risque :<br>LATENT | Probabilité estimée : 15% | Impact coût :<br>NIV. II | Impact délai :<br>NIV. III | Impact VA :<br>NIV. IV |
| Actions de surveillance du risque : | | | | |
| Actions préventive :<br>• Trouver des concurrents lorsque c'est possible | | | | |
| Actions correctives : | | | | |

| **Projet :** CLOUDIFY | | **Risque :** Bug dans le code source | | |
|---|---|---|---|---|
| Date d'identification : 22/05/2019<br>Responsable du risque :<br>Jonathan HAURAT | | **N°** : 9 | Famille de risques : Technique | |
| Description du risque :<br>Si le code source contient des erreurs, cela peut provoquer un risque de sécurité, ou avoir un impact sur toute l'activité du client. | | | | |
| Etat du risque :<br>LATENT | Probabilité estimée : 5% | Impact coût :<br>NIV. II | Impact délai :<br>NIV. III | Impact VA :<br>NIV. IV |
| Actions de surveillance du risque :<br>• Veille technique et sécuritaire | | | | |
| Actions préventive :<br>• Nous livrons l'avant-dernière version | | | | |
| Actions correctives : | | | | |

| **Projet :** CLOUDIFY | | **Risque :** Non-respect du CDCF | | |
|---|---|---|---|---|
| Date d'identification : 22/05/2019<br>Responsable du risque :<br>Jonathan HAURAT | | **N°** : 10 | Famille de risques : Qualitatif | |
| Description du risque :<br>Un non-respect du cahier des charges implique que le contrat passé avec le client n'a pas été tenu. L'entreprise sera pénalisée selon les termes du contrat en vigueur. | | | | |
| Etat du risque :<br>LATENT | Probabilité estimée : 10% | Impact coût :<br>NIV. III | Impact délai :<br>NIV. IV | Impact VA:<br>NIV. V |
| Actions de surveillance du risque : | | | | |
| Actions préventive :<br>• Outil de gestion de projet : Méthode Agile Scrum, fonctionnement sous forme de sprints. Ceci nous permet d'être le plus possible en phase avec le client. | | | | |
| Actions correctives : | | | | |

| **Projet :** CLOUDIFY | | **Risque :** Incendie | | |
|---|---|---|---|---|
| Date d'identification : 22/05/2019<br>Responsable du risque :<br>Jonathan HAURAT | | **N°** : 11 | Famille de risques : Naturel | |
| Description du risque :<br>Risque d'incendie interne (équipement électrique) ou externe (mégots de cigarette …) | | | | |
| Etat du risque :<br>LATENT | Probabilité estimée : 5% | Impact coût :<br>NIV. V | Impact délai :<br>NIV. V | Impact VA :<br>NIV. I |
| Actions de surveillance du risque :<br>• Système de détection d'incendie | | | | |
| Actions préventive :<br>• Extincteur dans les salles serveur et les couloirs<br>• Systèmes d'extinction automatisés d'incendie | | | | |
| Actions correctives :<br>• Système d'extinction d'incendie | | | | |

| **Projet :** CLOUDIFY | | **Risque :** Inondation | | |
|---|---|---|---|---|
| **Date d'identification :** 22/05/2019<br>Responsable du risque :<br>Jonathan HAURAT | | **N°** : 12 | Famille de risques : Naturel | |
| Description du risque :<br>Risque d'inondation à cause de fortes pluies | | | | |
| Etat du risque :<br>LATENT | Probabilité estimée : 1% | Impact coût :<br>NIV. V | Impact délai :<br>NIV. V | Impact VA:<br>NIV. I |
| Actions de surveillance du risque : | | | | |
| Actions préventive : | | | | |
| Actions correctives : | | | | |

## XII - Evaluation des risques

### Evaluation des niveaux « bruts » de risque

Nous qualifions de « niveaux bruts » le risque inhérent à une menace si aucune mesure de sécurité n'est implémentée.

| Risques | Gravité | Vraisemblance |
|---|---|---|
| Malveillance | Critique | Possible |
| Indisponibilité de ressources | Critique | Très improbable |
| Erreur de manipulation | Limitée | Possible |
| Mauvaise gestion de projet | Critique | Très improbable |
| Evolution des prix d'achat du matériel | Limitée | Improbable |
| Manque de compétences de l'administrateur | Importante | Très improbable |
| Panne matérielle | Limitée | Improbable |
| Défaillance d'un fournisseur clé | Limitée | Improbable |
| Bug dans le code source | Limitée | Très improbable |
| Non-respect du CdCF | Critique | Très improbable |
| Incendie | Critique | Très improbable |
| Inondation | Critique | Extrêmement improbable |

### Evaluation des niveaux de risque après application des protections

| Risques | Gravité | Vraisemblance |
|---|---|---|
| Malveillance | Importante | Improbable |
| Indisponibilité de ressources | Limitée | Très improbable |
| Erreur de manipulation | Limitée | Improbable |
| Mauvaise gestion de projet | Importante | Très improbable |
| Evolution des prix d'achat du matériel | Limitée | Très improbable |
| Manque de compétences de l'administrateur | Limitée | Extrêmement improbable |
| Panne matérielle | Négligeable | Extrêmement improbable |
| Défaillance d'un fournisseur clé | Limitée | Très improbable |
| Bug dans le code source | Limitée | Extrêmement improbable |
| Non-respect du CdCF | Importante | Extrêmement improbable |
| Incendie | Importante | Très improbable |
| Inondation | Importante | Extrêmement improbable |

## XIII - Objectifs de sécurité

Le tableau ci-dessous permet de faire le point sur nos objectifs vis-à-vis des risques étudiés. Soit notre objectif est d'éviter un risque, et lorsque cela n'est pas possible, nous allons au moins essayer de réduire son impact et sa probabilité d'occurrence.

| Risques | Eviter | Réduire |
|---|---|---|
| Malveillance | | √ |
| Indisponibilité de ressources | | √ |
| Erreur de manipulation | √ | √ |
| Mauvaise gestion de projet | √ | √ |
| Evolution des prix d'achat du matériel | | √ |
| Manque de compétences de l'administrateur | √ | √ |
| Panne matérielle | √ | √ |
| Défaillance d'un fournisseur clé | √ | √ |
| Bug dans le code source | | √ |
| Non-respect du CdCF | √ | √ |
| Incendie | | √ |
| Inondation | | √ |

### Inventaire des mesures de sécurité

Le tableau récapitulatif ci-dessous associe, à chaque risque, la mesure permettant de limiter ses effets. Les trois dernières colonnes indiquent la nature de la mesure de sécurité.

| Mesure de sécurité | Biens | Malveillance | Indisponibilité de ressources | Erreur de manipulation | Mauvaise gestion de projet | Evolution des prix | Manque de compétences | Panne matérielle | Défaillance fournisseur | Bug dans le code source | Non-respect du CdCF | Incendie | Inondation | Prévention | Protection | Récupération |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Pare-feu, IPS/IDS, ACL | Accès réseaux | √ | | | | | | | | | | | | √ | √ | |
| Restriction d'accès par filtrage MAC/IP | Accès réseaux | √ | | | | | | | | | | | | √ | | |
| Chiffrement des échanges de données | Accès réseaux | √ | | | | | | | | | | | | | √ | |
| Caméras de surveillance | Hébergement | √ | | | | | | | | | | | | √ | | |
| Serrures, portes de sécurité | Hébergement | √ | | | | | | | | | | | | √ | | |
| Matériel redondant | Hébergement Accès réseaux | | √ | | | | | √ | | | | | | √ | √ | |
| Sauvegardes | Hébergement | | √ | √ | | | √ | √ | | | | √ | √ | | | √ |
| Outils de gestion | Compétences Projet | | √ | | √ | | | | | | | | | √ | √ | |
| Réunions de projet | Projet | | √ | | √ | | | | | | √ | | | | √ | |
| Veille marketing | Projet | | | | | √ | | | | | | | | √ | | |
| Formations aux administrateurs | Compétences | | | √ | | | √ | | | | | | | √ | | |
| Documentation utilisateurs/admin | Compétences | | | √ | | | √ | | | | | | | √ | | |

| Mesure de sécurité | Biens | Malveillance | Indisponibilité de ressources | Erreur de manipulation | Mauvaise gestion de projet | Evolution des prix | Manque de compétences | Panne matérielle | Défaillance fournisseur | Bug dans le code source | Non-respect du CdCF | Incendie | Inondation | Prévention | Protection | Récupération |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Appel à la concurrence | Services | | | | | | | | √ | | | | | √ | √ | |
| Utilisation de la version N-1 | Plateforme OpenStack | | | | | | | | | √ | | | | | √ | |
| Systèmes de détection d'incendie | Hébergement | | | | | | | | | | | √ | | √ | | |
| Systèmes d'extinction d'incendie | Hébergement | | | | | | | | | | | √ | | | √ | |

## XIV - Produits dérivant de l'étude EBIOS

### Politique de sécurité

Les règles de sécurité énoncées ci-dessous constituent la politique de sécurité régissant l'infrastructure OpenStack qui sera mise en place :

| Sujet | Mesures de sécurité |
|---|---|
| Politique générique de sécurité | • La politique de sécurité doit exister<br>• La politique de sécurité doit être tenue à jour |
| Identification des besoins de confidentialité | • Les niveaux de confidentialité devant être appliqués sur chaque ressource doivent être clairement identifiés |
| Normes de sécurité des réseaux | • Les accès entrants doivent être filtrés, authentifiés, validés et journalisés.<br>• Les accès doivent être protégés par des mots de passes suffisamment puissants, et qui doivent être modifiés régulièrement |
| Organisation administrative | • Le client, les prestataires et les sous-traitants doivent s'engager à respecter la politique de sécurité<br>• La désignation de responsables de sécurité est nécessaire |
| Arrivée d'un nouveau collaborateur | • Un engagement de confidentialité doit être signé par le nouveau collaborateur |
| Départ d'un collaborateur | • Les identifiants de connexion du collaborateur doivent être réinitialisés à son départ |
| Durant l'exercice des fonctions d'un collaborateur | • Chaque collaborateur doit régulièrement être sensibilisé aux divers risques qui pèsent sur le SI<br>• Chaque collaborateur doit recevoir une formation adéquate à l'utilisation des outils métiers |
| Contraintes d'exploitation | • Tout service inexploité sur l'infrastructure doit être stoppé, et les ports associés doivent être fermés<br>• L'intégrité et l'efficacité des sauvegardes doit être vérifiée et validée très régulièrement (sur un rythme hebdomadaire dans le pire cas de figure)<br>• Le système de sauvegarde doit inclure des sauvegardes sur un site externe en vue d'une reprise d'activité après un incident affectant l'intégralité du site primaire<br>• Chaque modification prévue sur l'infrastructure doit d'abord être testée et documentée sur une infrastructure d'essais |
| Journalisation | • Tout évènement survenant sur le système d'informations (établissement d'une |

| | |
|---|---|
| | connexion, tentatives d'accès, modification de données, etc.) doit être journalisé sur un serveur dédié, et les journaux doivent être conservés pour une durée suffisante |
| Chiffrement | • Les échanges de données, ainsi que les supports de stockage doivent être chiffrés au moyen d'algorithmes sûrs |
| Assurances | • Les parties concernées doivent souscrire à un programme d'assurance adéquat garantissant les meilleures conditions de reprise d'activité en cas de sinistre |

# XV – Plan de continuité d'activité

## Définition et mise en situation

Le Plan de Reprise d'Activité, ou **PRA**, est un document décrivant des mesures de reprise d'activité en cas de sinistre. Toute indisponibilité étant synonyme de perte de revenus pour une entreprise, la reprise d'activité se doit d'être aussi rapide que possible, en s'assurant de restaurer en premier les ressources les plus critiques.

La solution étudiée dans notre étude concerne une suite logicielle supportée par un ensemble de briques physiques, que nous rassemblons comme tel :

1. Serveurs et stockage
2. Composants réseaux

Nous cherchons à éviter à tout prix toute indisponibilité, partielle ou totale, de l'une de ces trois briques, ce qui nous conduit à l'élaboration des scénarii suivants.

### Solutions de continuité/reprise d'activité - Infrastructure matérielle

Dans tous les cas de figure décrits ci-dessous, nous considérons comme acquis le fait qu'il existe au strict minimum un système de sauvegardes incrémentielle hébergé sur site.

#### *PHYS-N°1 : Présence de matériels de rechange sur site*

Une première solution pour l'entreprise serait d'acquérir des pièces de rechange, que ce soit des pièces détachées ou des serveurs complets, et de les conserver sur le même site que le site de production.

##### Avantages

- Reprise d'activité potentiellement rapide suivant la nature de l'incident
- Solution relativement peu onéreuse
- Configuration initiale peu complexe

##### Inconvénients

- Impose à l'entreprise d'assurer le stockage et l'inventaire des pièces de rechanges
- Solution totalement inefficace en cas de sinistre majeur (incendie), qui détruirait également les pièces de rechange
- Si la quantité de pièces de rechange d'un certain type est insuffisante, la reprise d'activité après incident peut prendre beaucoup plus de temps que prévu
- A moins que le matériel n'ait été configuré à l'avance, la reprise d'activité pourrait prendre du temps
- Solution impossible à automatiser

##### Implémentation type de la solution

Au moment de la mise en service du produit, des pièces supplémentaires peuvent être livrées et stockées en lieu sûr dans les locaux hébergeant la solution. Ainsi, en cas de défaillance d'un matériel disposant d'une pièce de rechange, le remplacement peut être effectué rapidement.

##### Limitations de la solution

Cette solution ne fournit presque aucune protection contre la perte de données ou d'accessibilité. En effet, nous sommes ici dans une solution relevant du ***Curatif***, car ce n'est qu'une fois qu'un problème (en l'occurrence ici, une défaillance matérielle) s'est déclaré qu'il est possible d'agir. De plus, si aucune autre solution de continuité et/ou de reprise d'activité n'est implémentée, toute défaillance provoquera une perte de données et/ou d'accessibilité.

##### Chiffrage de la solution

En règle générale, suivant la quantité et le type de matériels de rechange commandés, le prix de cette solution varie de 15% à 30% du coût total du matériel. Nous sommes ici dans un financement de solution de type « achat unique », à renouveler si nécessaire en cas d'utilisation d'un matériel de rechange. *Chiffrage possible sur devis*.

*PHYS-N°2 : Sauvegarde de données*

Une autre solution élémentaire mais très efficace serait d'intégrer des solutions de sauvegarde pour les données jugées importantes. Une telle sauvegarde peut être effectuée sur des supports externes situés sur site, ou vers un hébergement Cloud prévu à cet effet.

#### Avantages

- Solution pouvant être relativement peu onéreuse
- Fourni une base indispensable à tout plan de reprise sur incident
- Cette solution peut être automatisée
- De très nombreuses solutions de sauvegarde existent, et peuvent être combinées pour renforcer l'efficacité de la protection

#### Inconvénients

- En cas de sauvegarde sur site, une perte de données est à envisager en cas d'attaque informatique ou de sinistre des locaux
- Pour une sauvegarde externe, et suivant le volume de données à sauvegarder, il peut être nécessaire de dédier une connexion internet haut-débit
- Il est nécessaire de surveiller activement et régulièrement le bon fonctionnement des systèmes de sauvegarde

#### Implémentation type de la solution

De manière générale, le nombre et la nature des sauvegardes dépendent directement de l'importance des données que l'on veut protéger. Le tableau suivant illustre cette notion avec des valeurs « habituelles » :

| Criticité de la donnée | Nombre recommandé de sauvegardes | Planification recommandée | Nature de la sauvegarde |
|---|---|---|---|
| Critique | 3 | Quotidienne | Complète, site externe |
| | | Biquotidienne | Incrémentielle, site externe |
| | | Biquotidienne | Incrémentielle, sur site |
| Importante | 2 | Quotidienne | Incrémentielle, sur site |
| | | Hebdomadaire | Complète, site externe |
| Moyennement importante | 1 | Hebdomadaire | Incrémentielle, sur site |
| Peu importante | 1 | Mensuelle | Complète, sur site |

### Limitations de la solution

Les supports de sauvegardes étant utilisés régulièrement, ils sont soumis à une certaine usure pouvant provoquer leur dysfonctionnement, il faut donc contrôler régulièrement les résultats de sauvegarde. De plus, si tous les supports de sauvegarde se trouvent sur le site de production, et que ce dernier se trouve sinistré, les données risquent d'être perdues.

### Chiffrage de la solution

Le chiffrage dépend entièrement du volume de données à sauvegarder, du nombre et de la nature des copies à conserver, si la sauvegarde se fait sur site ou hors site, et du support de sauvegarde choisi. *Chiffrage possible sur devis.*

*PHYS-N°3 : Redondance et haute disponibilité sur site*

Dans ce cas, l'architecture matérielle et logicielle est doublée (voire plus), les configurations et données sont répliquées en temps réel de l'infrastructure « maître » à l'infrastructure « esclave », et tout arrêt de production sur le système principal est automatiquement compensé par les ressources du système secondaire. La mise en place d'une sauvegarde externe ajouterait une protection non-négligeable contre les éventuelles pertes de données, notamment en cas de cyberattaque.

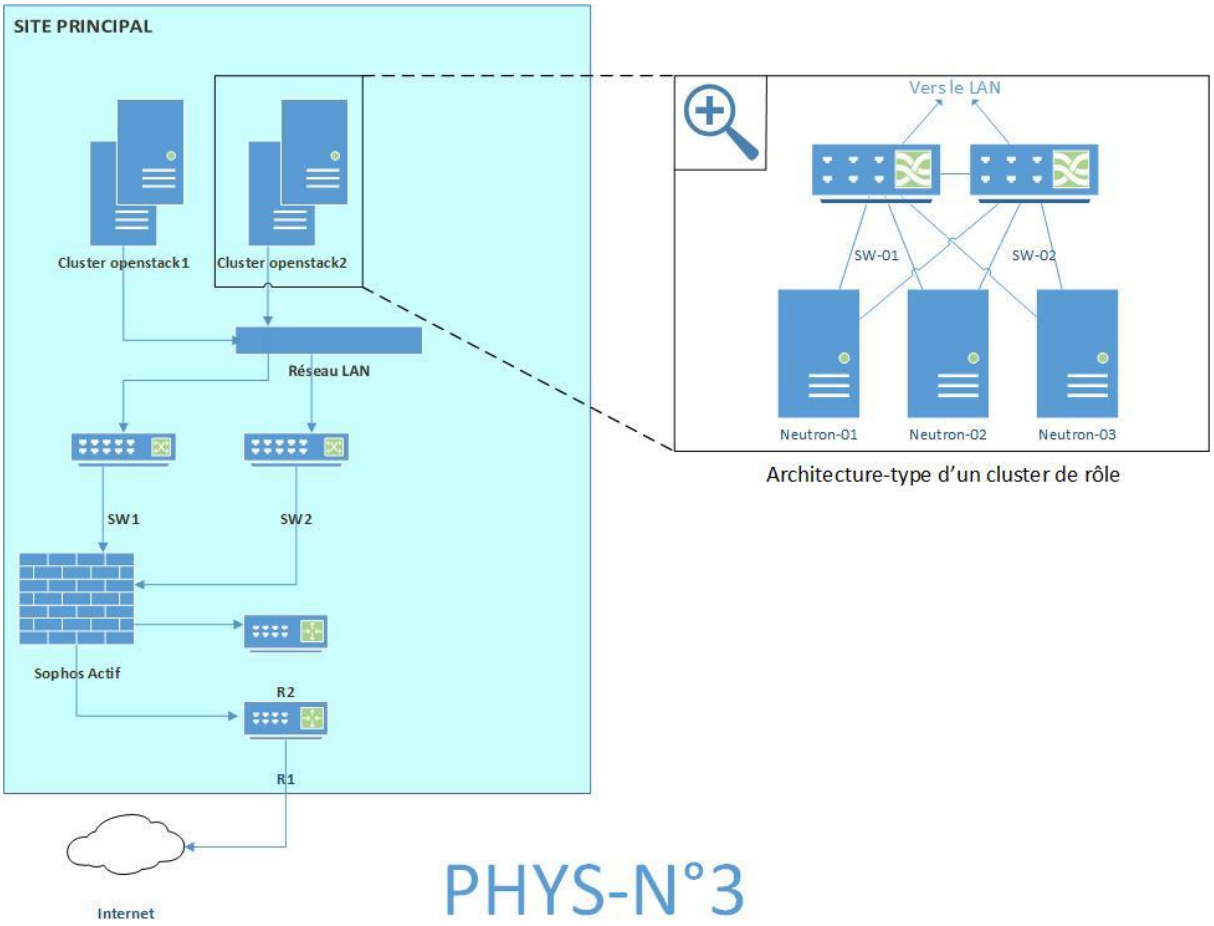



Figure 1 - Schéma de principe de la solution

### Avantages

- Reprise d'activité potentiellement très rapide, voire même instantanée

### Inconvénients

- Il s'agit d'une solution plus onéreuse que dans les deux premiers cas de figure
- Il faut prévoir de la place pour héberger le double de ressources, et assumer l'entretien et la consommation électrique de ces équipements supplémentaires
- Solution inefficace contre certains sinistres (incendie, inondation, certaines cyberattaques, négligence)
- Configuration initiale assez complexe

### Implémentation type de la solution

Selon l'accord conclut avec le client final, les éléments critiques de l'infrastructure pourront être commandés et installés en double exemplaire, avec une gestion logicielle assurant le basculement automatique vers le matériel de secours en cas de défaillance sur le matériel principal. Une autre configuration possible est de configurer ce matériel dédoublé en mode d'équilibrage de charge.

Parmi les éléments critiques, nous pouvons citer :

- Serveurs ;
- Systèmes de stockage ;
- Switches ;
- Routeurs.

### Limitations de la solution

Augmenter la quantité de matériel à acquérir a un impact évident sur le budget du projet. De plus, la configuration initiale est plus complexe à implémenter, et requiert plus de compétences de la part de l'équipe en charge de la réalisation technique. Enfin, même si cette solution offre un niveau acceptable de tolérance de panne, tout sinistre affectant les locaux (un incendie, par exemple) risque de détruire tous les matériels et les données qu'ils contiennent.

### Chiffrage de la solution

Le prix moyen d'une telle solution équivaut environ au prix total du matériel « minimum » permettant de répondre au cahier des charges. Ainsi, pour un projet dont le budget est de 100.000,00€, si le coût du matériel minimum est de 25.000,00€, alors le budget total du matériel et de l'implémentation de cette solution de continuité d'activité atteindra environ 50.000,00€. Nous sommes là encore sur un plan de financement de type « achat unique » pour le matériel double, plus un abonnement mensuel, trimestriel ou annuel pour les frais de maintenance de la solution de haute disponibilité. *Chiffrage possible sur devis.*

*PHYS-N°4 : Redondance et haute disponibilité sur site, plus réplication en temps réel vers un site de secours*

Cette solution est de loin la plus onéreuse et la plus complexe à mettre en œuvre, mais le niveau de sécurité qu'elle procure vis-à-vis d'une perte de productivité sur incident est extrêmement élevé. Ainsi, le site principal fournit une première couche de sécurité en ayant du matériel hautement redondant et disponible (disques configurés en RAID, clusters de basculement, pièces de rechanges), prévenant ainsi les pertes d'activité en cas de défaillance matérielle ou logicielles localisée. De plus, la liaison avec au moins un site de secours, et la réplication en temps réel vers ce dernier des données et configurations (via un canal sécurisé, bien entendu) permet de rapidement reprendre une activité normale si un sinistre majeur devait totalement détruire le site principal.

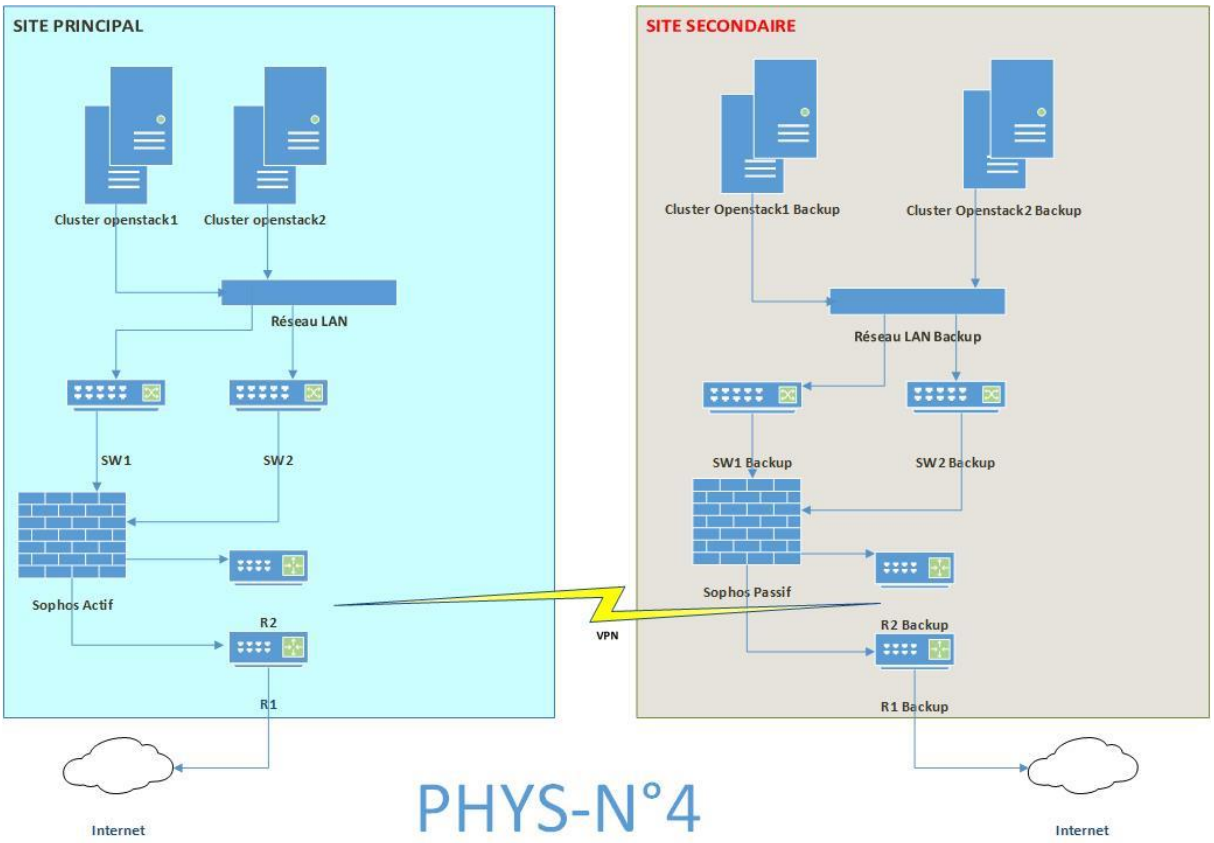



Figure 2 - Schéma de principe de la solution

Plusieurs systèmes de sauvegarde répartis entre les différents sites augmenteront encore sensiblement le niveau global de protection apporté par cette solution.

### Avantages

- Le plus haut niveau de tolérance de panne que l'on puisse imaginer
- Reprise d'activité potentiellement très rapide, voire même instantanée
- Procédures de reprise d'activité relativement simples à mettre en œuvre
- Solution insensible aux catastrophes localisées

### Inconvénients

- Solution très onéreuse
- Nécessite d'avoir une excellente connexion internet, possiblement redondée elle aussi, et un canal de communication sécurisé doit être établi
- Configuration initiale complexe
- Maintenance assez complexe

### Limitations de la solution

Afin de pouvoir fonctionner dans les meilleures conditions, et de pouvoir assurer un niveau optimal de reprise sur incident, une telle solution nécessite une réplication en temps réel de l'intégralité des données du site de production vers un site de secours, qui doit lui-même abriter une architecture informatique identique à celle du site primaire. Au moins une liaison internet fiable et de très haut débit est requise pour assurer cette réplication en temps réel.

### Chiffrage de la solution

Cette solution est de loin la plus coûteuse -aussi bien à implémenter qu'à maintenir-, car elle nécessite de dédoubler l'infrastructure de production, de l'héberger sur un site distant, et d'avoir au moins une connexion internet dédiée à très haut débit pour assurer la réplication continue des données vers le site de secours.

Ainsi, cette solution nécessite non seulement un investissement initial important, auquel s'ajoutent des frais mensuels de location en datacenter et au moins abonnement pour une fibre optique dédiée. *Chiffrage possible sur devis*.

### Solutions de continuité/reprise d'activité - Solution CLOUDIFY

Nous proposons diverses solutions pour assurer la reprise ou la continuité d'activité sur notre solution logicielle CLOUDIFY. Certaines de ces solutions ont toutefois des prérequis qu'il faut respecter, sans quoi il ne sera pas possible de les implémenter :

#### *LOG-N°1 : Sauvegarde complète des bases de données et configurations des services*

Cette mesure de reprise d'activité consiste à exporter régulièrement une copie complète des données et fichiers de configuration de la solution vers un support dédié.

##### Prérequis

- Présence d'une solution de sauvegarde, sur site ou hors site, à même de recevoir le volume de données que représente CLOUDIFY et les données générées par ses utilisateurs

##### Avantages

- En cas de problème majeur, qu'il s'agisse d'une défaillance matérielle, d'un acte de malveillance ou d'une erreur humaine, il est possible de restaurer des données saines à partir de la dernière sauvegarde
- La sauvegarde peut être automatisée

##### Inconvénients

- En cas de problème, toutes les données produites depuis la dernière sauvegarde seront perdues. Il faut alors déterminer le **RPO** (**R**ecovery **P**oint **O**bjective), c'est-à-dire la quantité de données qu'il est acceptable de perdre, et configurer l'intervalle de sauvegardes en conséquences
- La restauration après incident peut être partiellement automatisée, mais une intervention humaine reste nécessaire pour finaliser le retour à la normale
- Une surveillance accrue de la sauvegarde doit être mise en place afin d'éviter une perte totale de données

##### Chiffrage de la solution

Si des supports de sauvegarde sont mis à notre disposition, nous allons systématiquement implémenter cette solution gratuitement.

*LOG-N°2: Clustering de services*

Cette mesure de continuité d'activité a pour objectif de répartir la charge de travail des différents composants logiciels sur plusieurs supports physiques distincts.

#### Prérequis

- Disposer d'au moins deux fois plus de serveurs que ce qui est requis pour monter une infrastructure minimale
- Une redondance des matériels actifs du réseau (switches et routeurs) serait un plus
- En cas de redondance vers un site externe, une liaison montante dédiée de bonne qualité sera requise

#### Avantages

- La charge de travail étant répartie sur un plus grand nombre de machines, les performances globales du système s'en trouveront améliorées
- En cas de défaillance d'un composant ou d'un serveur complet, le service qu'il assurait ne sera que faiblement impacté, étant encore maintenu par un autre nœud
- Configuration initiale relativement simple pour une redondance sur site
- En cas de défaillance, un matériel peut assez facilement être remplacé en lui appliquant la configuration adéquate (tâche facilitée en cas d'implémentation de la solution N°1)
- La redondance des données peut se faire vers un site externe, réduisant énormément le risque de perte de données en cas de sinistre affectant le site primaire

#### Inconvénients

- Solution indirectement onéreuse, car elle requiert une architecture matérielle de haute disponibilité pour être implémentée. Son prix est directement lié au niveau de redondance désiré
- La mise en place d'une redondance vers un site externe est plus complexe

#### Chiffrage de la solution

Si une infrastructure redondante est mise à notre disposition, quel que soit le nombre de nœuds dans le cluster, nous implémenterons gratuitement cette solution.

## XVI – Conclusion

Nous avons pu voir que de nombreux risques, d'origines diverses et variées, pèsent sur l'infrastructure du système d'information supportant notre solution, ainsi que sur la solution logicielle elle-même.

A ce titre, nous recommandons vivement la mise en place de mesures préventives qui permettraient d'éviter des arrêts imprévus du système. De plus, compte tenu de la complexité du système considéré, ainsi que du volume important de données et d'utilisateurs qu'il supportera, nous vous conseillons fortement d'opter au minimum pour la solution **PHY-N°2**, et de la dimensionner pour être en adéquation avec l'importance des données gérées par **CLOUDIFY**, et optionnellement de la combiner à la solution **PHY-N°1**.

Nous recommandons également, dans un premier temps au moins, d'opter pour la solution **PHY-N°3** présentée ci-dessus, et de la faire ensuite évoluer vers la solution **PHY-N°4** si vous jugez cela nécessaire.

Aussi, les solutions présentées au paragraphe précédent ne décrivent que de manière générique des méthodes de protection contre la perte d'activité. Il est possible d'établir des solutions intermédiaires, faites sur mesure, afin de trouver le juste équilibre entre la charge budgétaire et le niveau de protection fourni.

Concernant la prévention et la reprise sur incident au niveau logiciel, tout achat d'une solution CLOUDIFY vous rend éligible à une implémentation gratuite des solutions **LOG-N°1** et **LOG-N°2**, à condition que les prérequis respectifs de ces solutions soient respectés.