**Projet Annuel 3SRC Groupe 5**

**1 : Description et rôle de chaque personne**

MENAGER Ewan :

LUIGI Theo :

JACQUEL Angel :

NABAJOTH Gilles :

1: Ewan : infra réseau (switch / solution de messagerie / Serveur sylogs / et transferts à chaud des VM / liason VPN)

2: Théo : Mise en place de l'AD / GPO / réplication d'AD / Mise en place de la virtualisation / serveur de supervision, redondance des VM

3: Gilles : infra sécu (routeur / règle de filtrage / téléphonie IP / accès téléphonie IP sur Smartphone)

4: Angel: Stockage / partage de fichier / sauvegarde / Mise en place ESXI / gestion vCenter/ vSphere Replication

**2 : Expression du besoin :**

***Qu'est-ce que le projet Kasgrunt:***

***Kasgrunt est une entreprise spécialisée dans la fourniture de bureau, elle est l’un des leaders français du secteur. Elle contient deux sites, un principal, un à Paris et l’autre à Reims. La société Kasgrunt souhaite mettre en place un site distant qui leur sert de redondance en cas de panne entre la liaison Paris-Reims. Elle souhaite mettre en place une infrastructure complète avec une tolérance aux pannes, ainsi qu'un système de sauvegarde des données. Pour son besoin, la société Kasgrunt fournit le cahier des charges suivant :***

1. Sécurité et résilience  
   Kasgrunt cherche une infrastructure capable de résister aux pannes matérielles et aux interruptions de services grâce à une redondance de panne. Elle souhaite également une sécurité au niveau des données c’est pour cela qu’un infrastrure de sauvegarde est à prévoir.
2. Gestion centralisée des utilisateurs  
   Un nom de domaine et une structure de gestion d’utilisateurs centralisée (par exemple via Active Directory ou Azure AD) sont requis pour simplifier l’administration des accès et sécuriser les données.
3. Virtualisation et haute disponibilité  
   La société souhaite bénéficier d'une infrastructure virtualisée capable de maintenir la haute disponibilité. Une configuration avec VMware ESXi et vCenter est prévue, Un basculement à chaud des VM est nécessaires.
4. Sauvegarde, restauration des données et logs   
   Kasgrunt demande une solution de sauvegarde complète, incluant des sauvegardes incrémentielles et une fonctionnalité de type "time machine". De plus une solution de logs est prévue.
5. Sécurisation des connexions réseau et du filtrage d'accès  
   Des connexions sécurisées via VPN / IPSEC, une protection renforcée par firewall multicouche, et un filtrage d'accès sur l’infrastructure réseaux et serveur sont requis pour une utilisation professionnelle et une sécurité renforcée.
6. Communication et connectivité interne  
   Pour réduire les frais de communication entre ses deux sites principaux, Kasgrunt souhaite déployer une solution de téléphonie IP interne. La connectivité doit aussi permettre aux employés de se connecter depuis n’importe quel emplacement.
7. Supervision et métrologie  
   Kasgrunt souhaite pouvoir superviser l’état des équipements et des services, et recevoir des alertes en cas de défaillance. La surveillance de la performance des serveurs (métrologie) est également nécessaire pour assurer un suivi.

**3 : Planification du projet**

**2. Planification du projet et deadlines**

**Calendrier prévisionnel des phases du projet, visant à assurer une mise en place optimale et dans les temps pour la société Kasgrunt.**

**Phase 1 :** Préparation et planification détaillée

* + *Durée estimée : 2 semaines*
  + Activités :
    - Réunion initiale avec Kasgrunt pour confirmer les exigences.
    - Sélection des équipements, logiciels et configurations nécessaires.

**Phase 2 :** Installation et configuration des infrastructures réseau et sécurité

* + *Durée estimée : 4 semaines*
  + Activités :
    - Installation des équipements réseau (firewalls, VPN, VLAN).
    - Configuration de la redondance des firewalls et du routage pour sécuriser les communications inter-sites.

**Phase 3 :** Mise en place de l'infrastructure de virtualisation, de stockage et de logs

* + *Durée estimée : 8 semaines*
  + Activités :
    - Déploiement de serveurs VMware ESXi et de vCenter pour la gestion centralisée.
    - Mise en place d’un stockage SAN virtualisé avec clustering pour la haute disponibilité.

**Phase 4 :** Installation et configuration des solutions de sauvegarde

* + *Durée estimée : 3 semaines*
  + Activités :
    - Mise en place des solutions de sauvegarde pour les VM et les fichiers.
    - Configuration des sauvegardes incrémentielles et options de restauration pour assurer la protection des données.

**Phase 5 :** Mise en place des systèmes de communication et services utilisateurs

* + *Durée estimée : 3 semaines*
  + Activités :
    - Installation de la téléphonie IP et de la messagerie.
    - Déploiement d’une solution de partage de fichiers en local.

**Phase 6 :** Supervision et tests finaux

* + *Durée estimée : 4 semaines*
  + Activités :
    - Mise en place de la supervision et de la métrologie des services et du réseau.
    - Tests finaux de résilience et de sécurité pour validation de la solution.

**Phase 7 :** Formation et documentation

* + *Durée estimée : 3 semaines*
  + Activités :
    - Formation du personnel Kasgrunt pour la prise en main des outils.
    - Transmission des documents techniques et guides d'utilisation.

**4 : Analyse de risques :**

**Liaison VPN IPsec :**

* **Risque :**

1 : Coupure réseaux qui engendre la perte de la connexion VPN entre les deux sites / attaque Man in the middle.

* **Gravité :**

2 : une indisponibilité de la communication entre les deux sites plus possible vols / perte de données par une personne malveillante.

* **Vraisemblance :**

3 : la situation à une grande chance d’arriver si aucune solution de redondance et sécurité n’est mis en place.

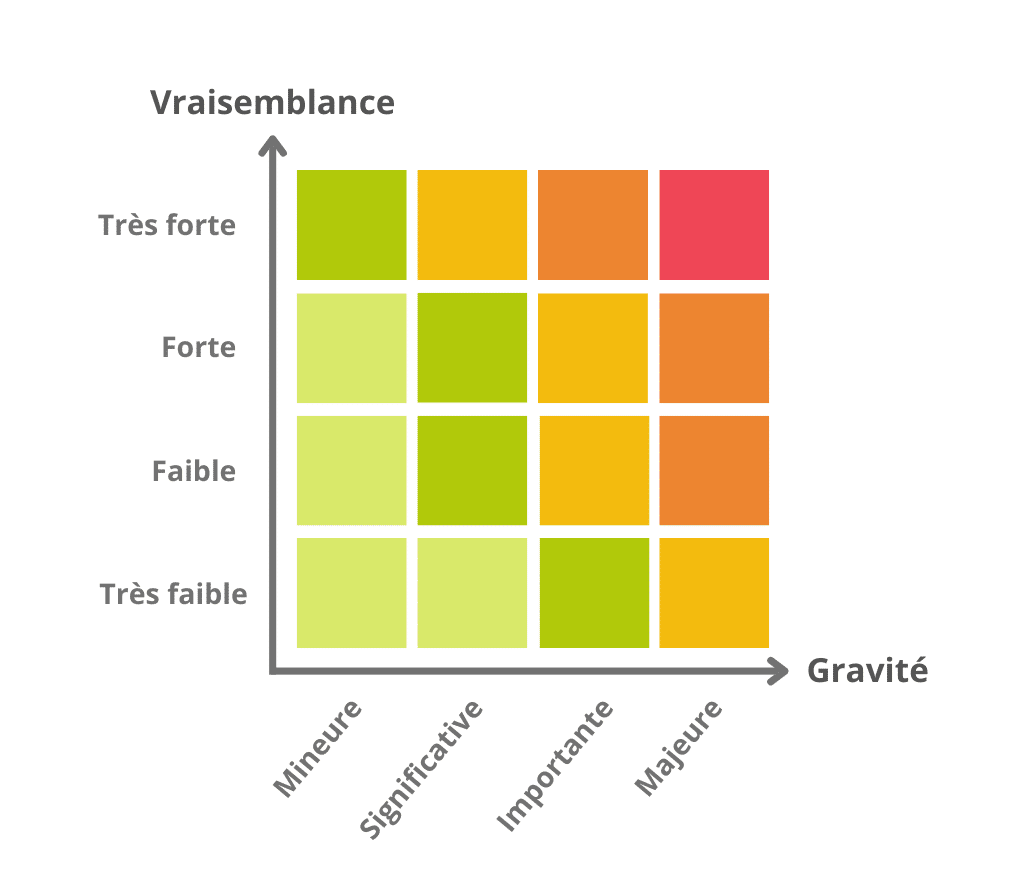


Figure 1: échelle de cotation risque

**Switching & VLAN :**

* **Risque :**

1 : perte de l’équipement / perte de communication entre les VLANs / perte de liaison entre deux switch / routeur / ***saut de VLAN***

* **Gravité :**

2 : indisponibilité / compromission des données / coût matériel / perte de données

* **Vraisemblance :**

3 : la situation à une grande chance d’arriver si aucune solution de redondance et sécurité n’est mis en place.

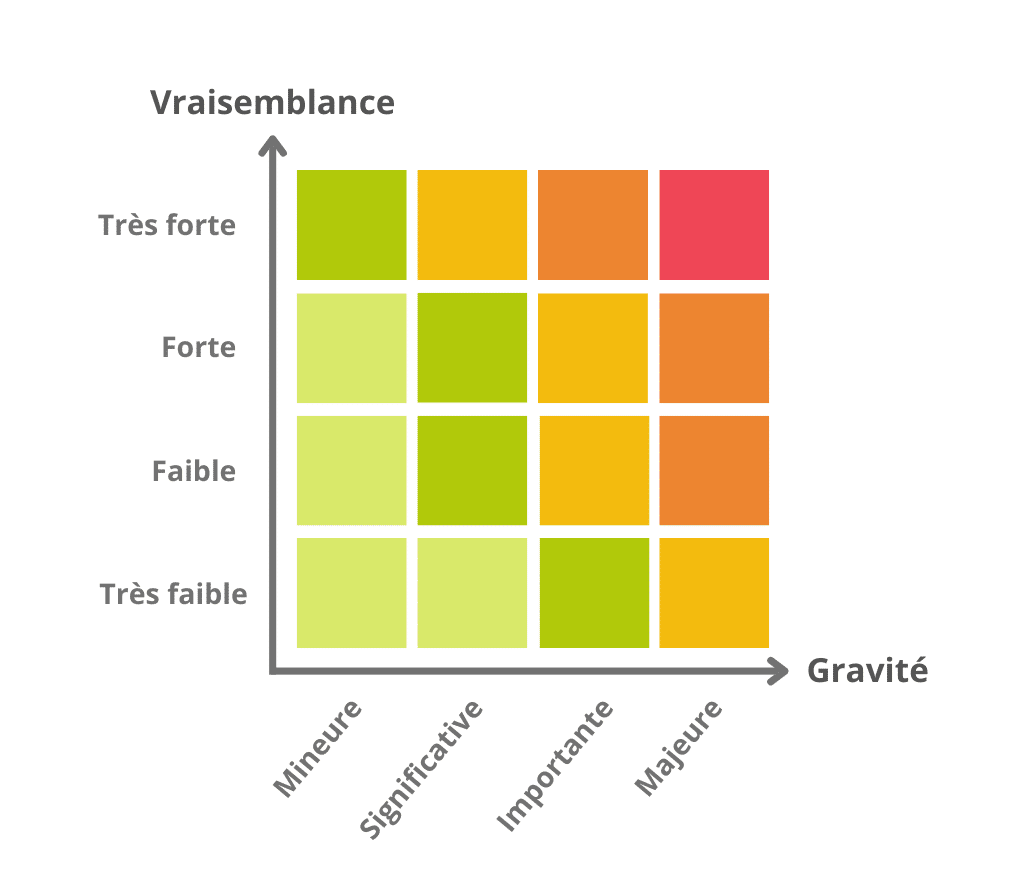


Figure 2: échelle de cotation risque

**Deux niveaux de firewall :**

* **Risque :**

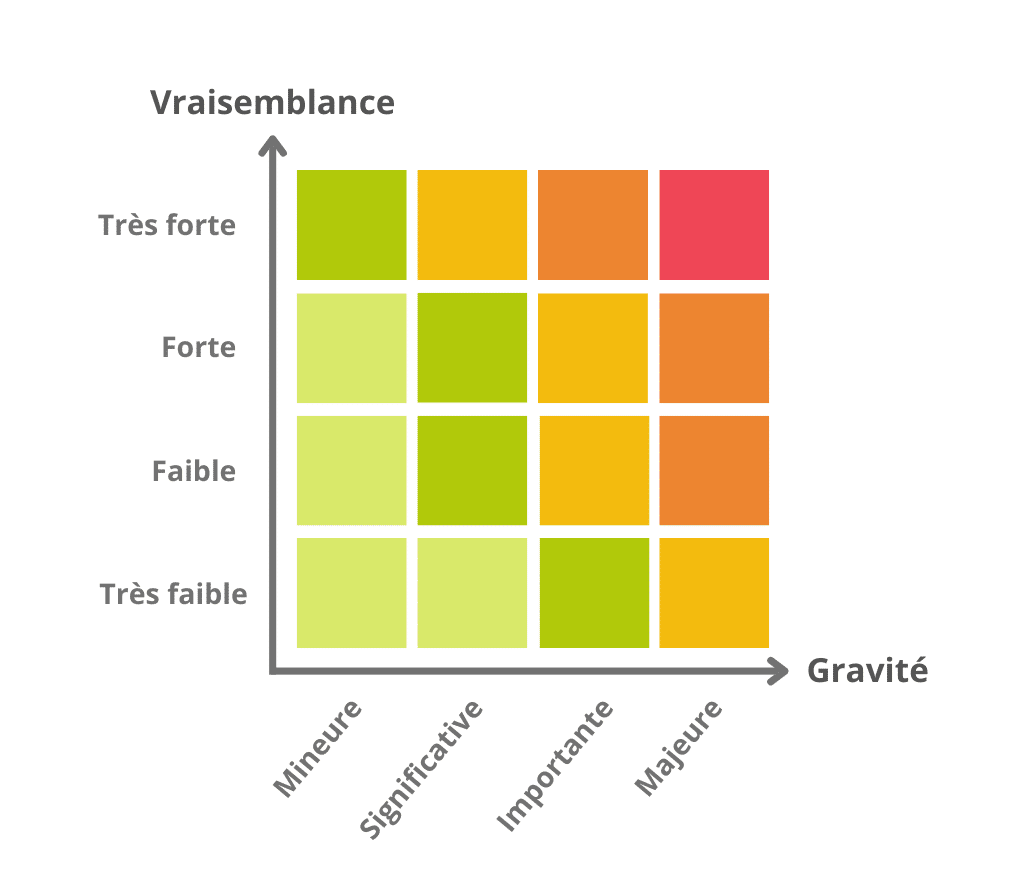
1 : perte de l’équipement / attaque par une personne malveillante à la suite d’une mauvaise configuration de la sécurité ou une faille à la suite d’une non-gestion des mises à jour.

* **Gravité :**

2 : indisponibilité / compromission des données / coût matériel / perte de données

* **Vraisemblance :**

3 : la situation est plausible, si celle-ci arrive elle peut engendrer un risque majeur pour l’entreprise.



**Redondance de firewalls :**

* **Risque :**

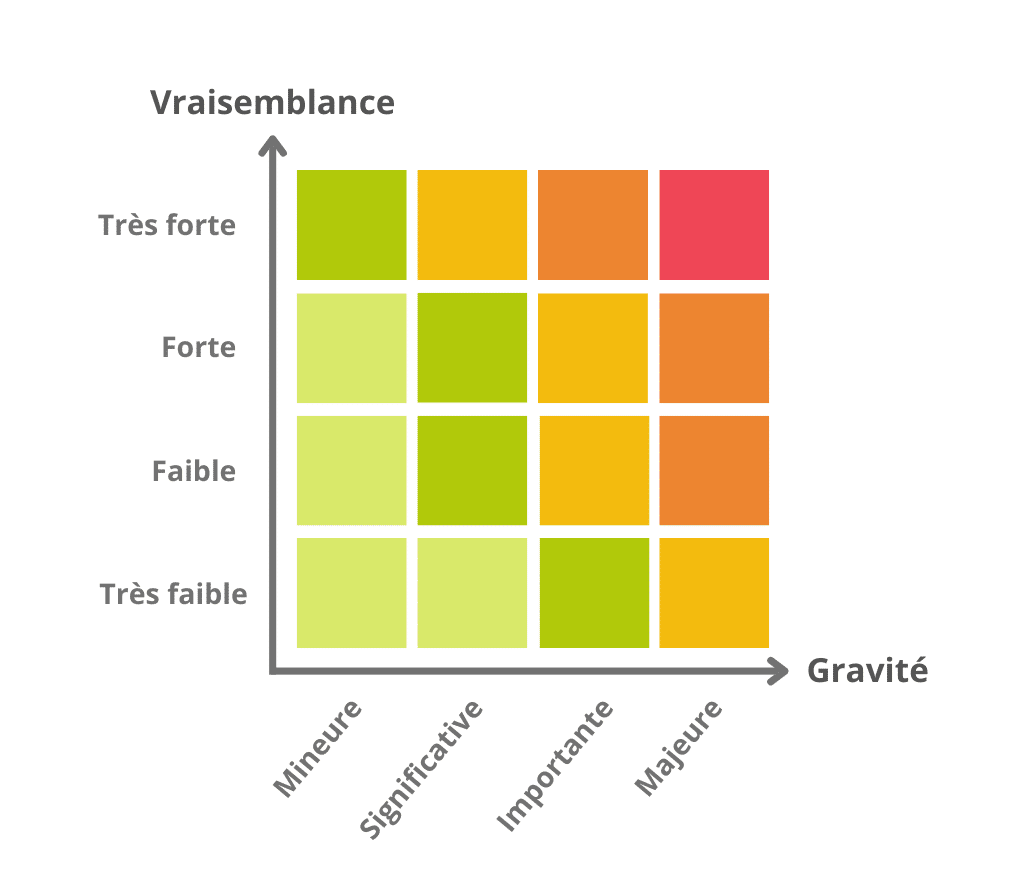
1 : Mauvaise configuration de la redondance / ce qui engendre une indisponibilité en cas de panne d’un des firewalls

* **Gravité :**

2 : indisponibilité

* **Vraisemblance :**

3 : la situation est peux probable est engendrais un risque significatif



**Routage avec les firewalls / routeurs Cisco:**

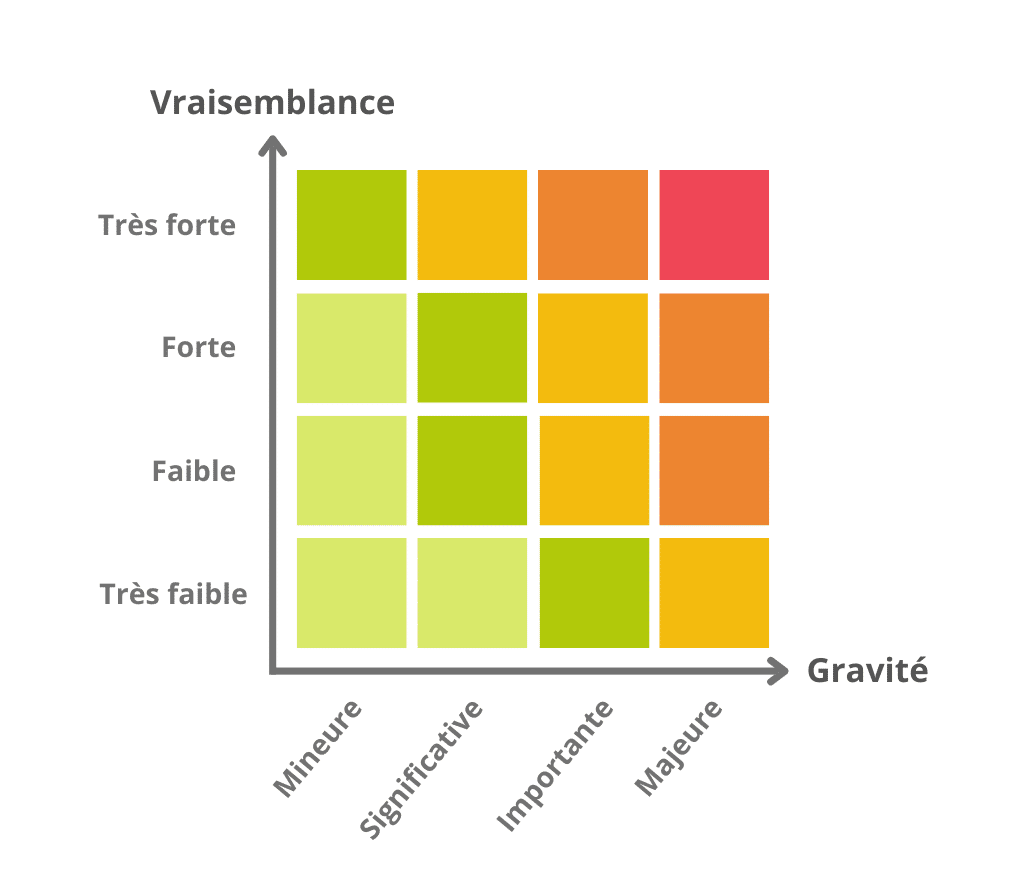
* **Risque :**

1 : perte d’un routeur ou d’un pare feux

* **Gravité :**

2 : indisponibilité

* **Vraisemblance :**

3 : la situation est plausible, si celle-ci arrive elle peut engendrer un risque significatif.   


**Serveurs:**

* **Risque :**

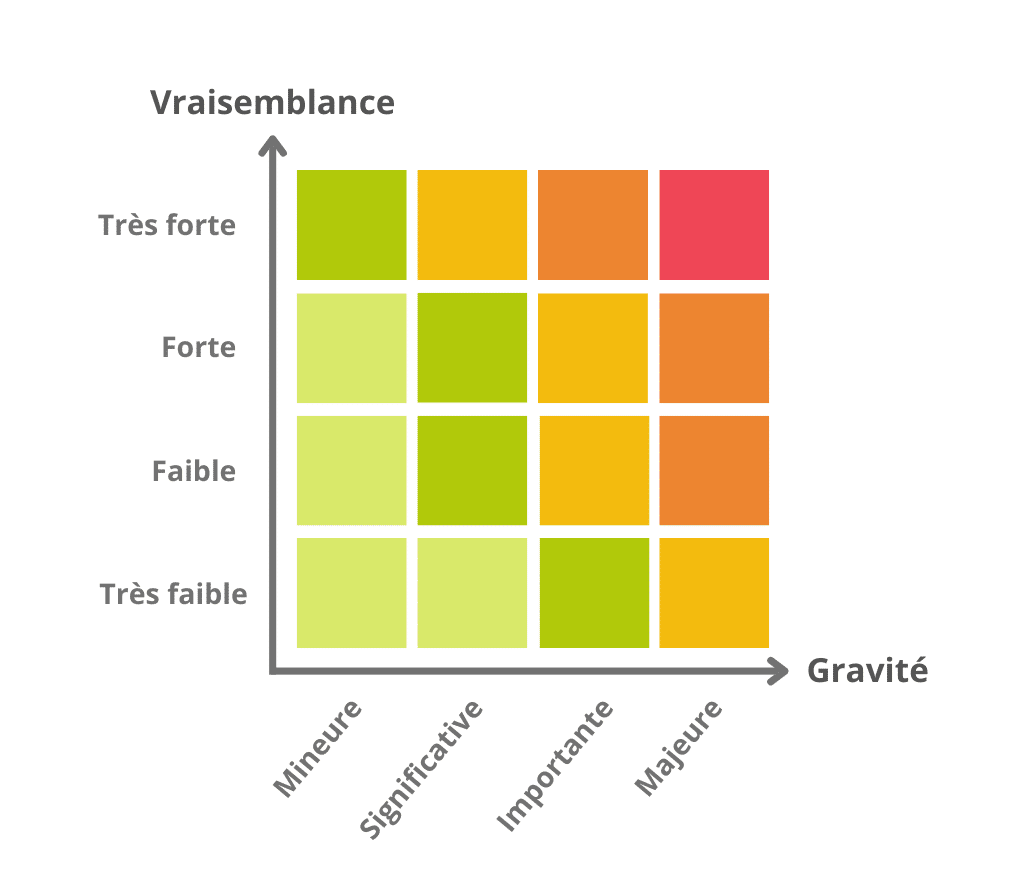
1 : perte d’un serveur / perte de données / attaque par malveillante / pertes ou corruption des VM / serveurs.

* **Gravité :**

2 : indisponibilité / perte de données / corruptions de données / vols de données / coûts matériel.

* **Vraisemblance :**

3 : la situation est plausible et engendrais des risques conséquents pour l’entreprise voir sans retour possible.



**Infrastructure sauvegarde :**

* **Risque :**

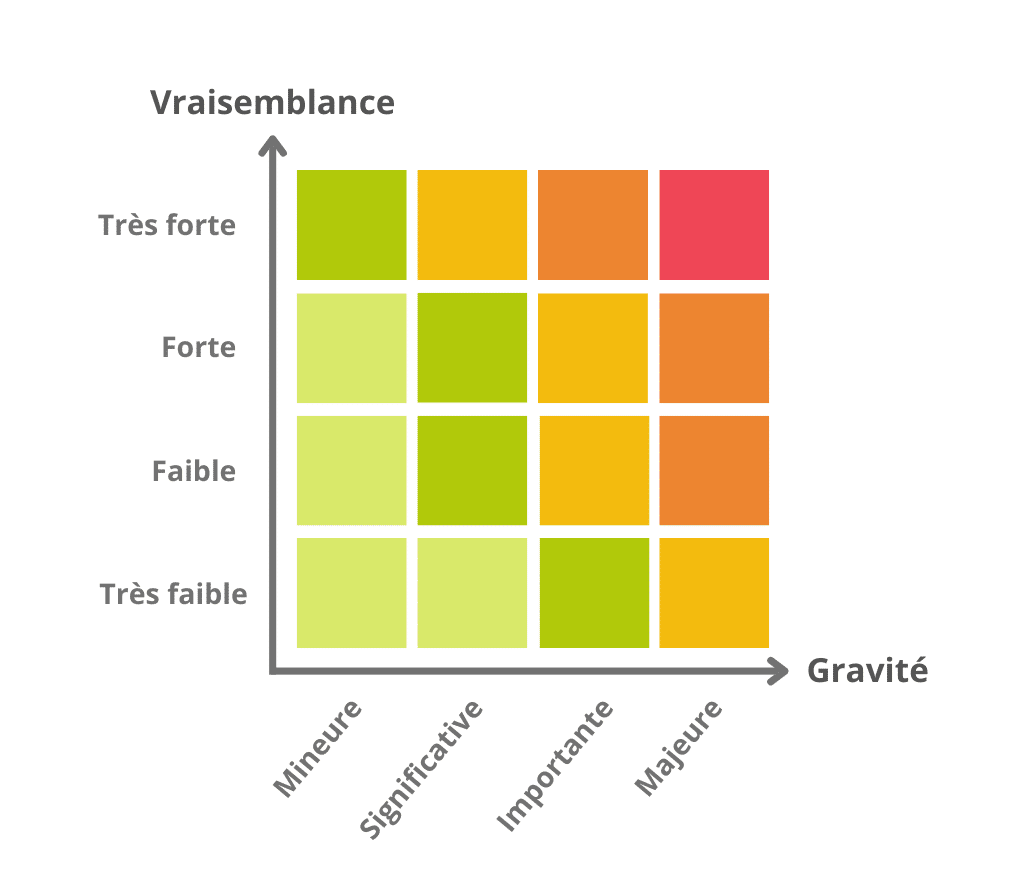
1 : perte du serveur/ perte de données / attaque par malveillante / perte d’un disque

* **Gravité :**

2 : indisponibilité / perte de données / corruptions de données / vols de données / coûts matériel.

* **Vraisemblance :**

3 : la situation est plausible et engendrais des risques conséquents pour l’entreprise voir sans retour possible.



**Infrastructure stockage :**

* **Risque :**

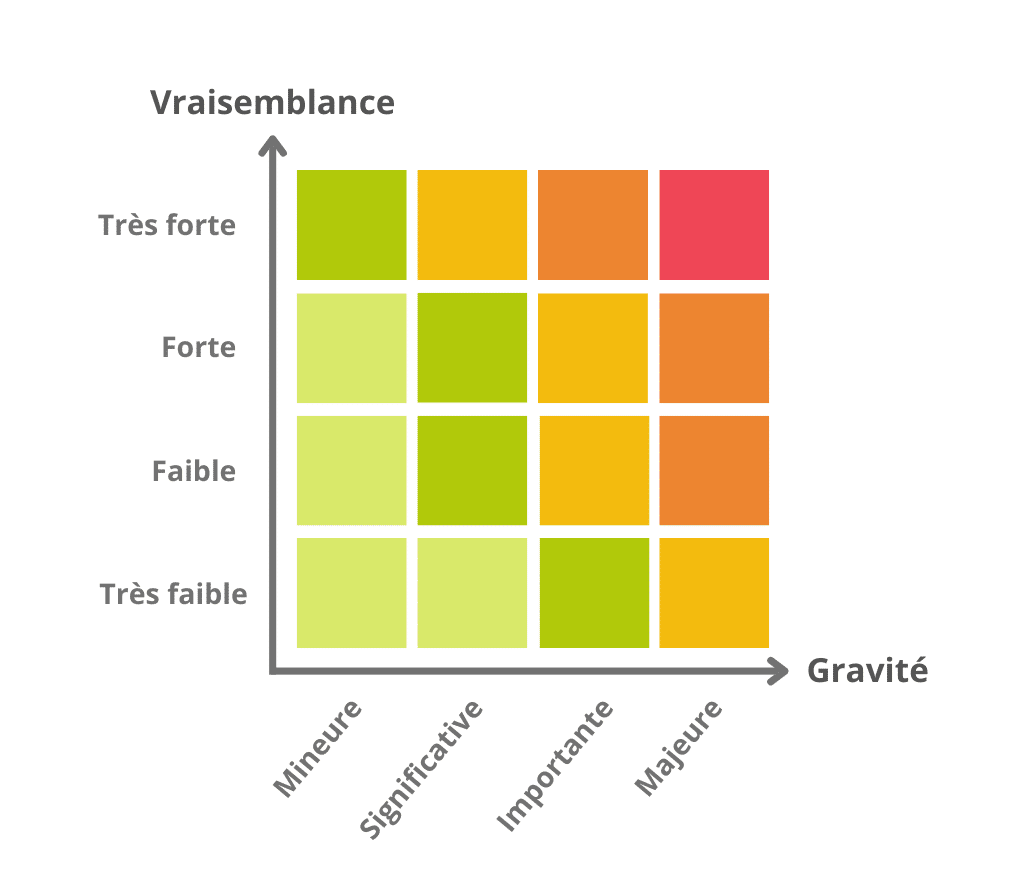
1 : perte du serveur/ perte de données / attaque par malveillante / perte d’un disque

* **Gravité :**

2 : indisponibilité / perte de données / corruptions de données / vols de données / coûts matériel.

* **Vraisemblance :**

3 : la situation est plausible et engendrais des risques conséquents pour l’entreprise voir sans retour possible.



**Serveurs AD / linux :**

* **Risque :**

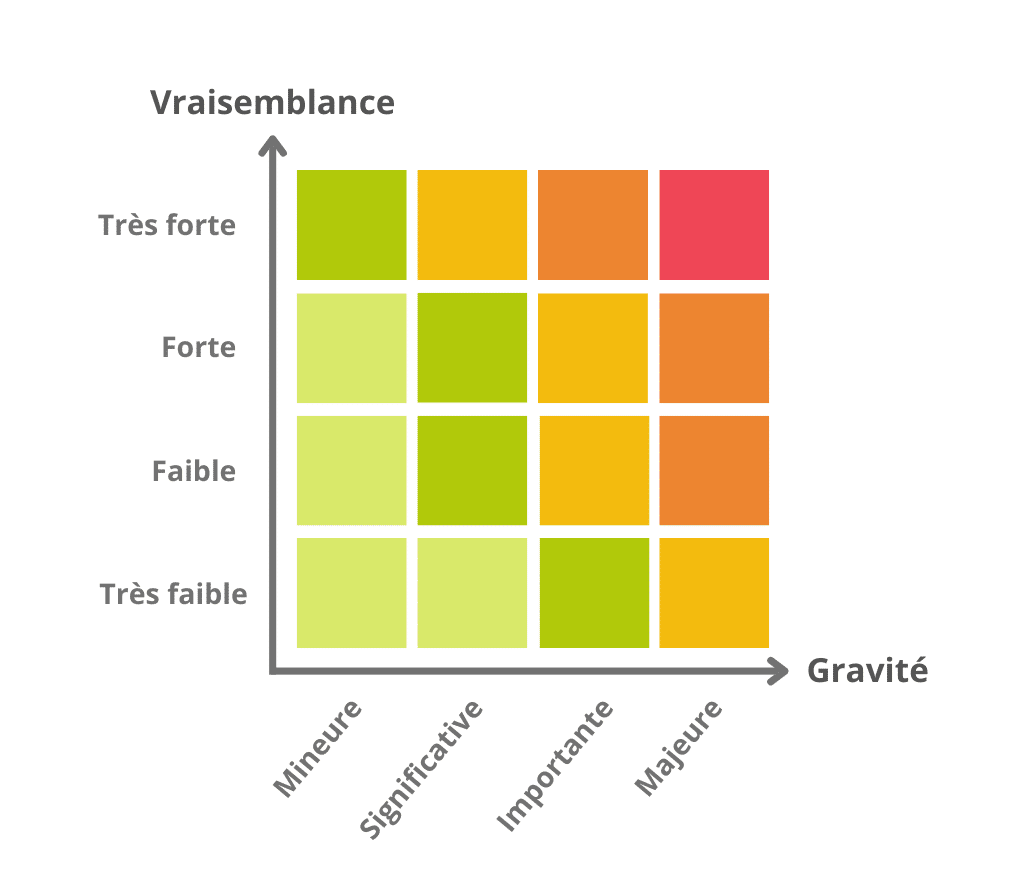
1 : perte d’un serveur / perte de données / attaque par malveillante / pertes ou corruption des VM / serveurs.

* **Gravité :**

2 : indisponibilité / perte de données / corruptions de données / vols de données / coûts matériel.

* **Vraisemblance :**

3 : la situation est plausible et engendrais des risques conséquents pour l’entreprise voir sans retour possible.



**Conclusion**

**Ce document constitue une première réponse à l’appel d’offre de Kasgrunt et présente notre compréhension du projet et des exigences associées. La solution proposée par ESGI Consulting vise à offrir une infrastructure stable, résiliente et sécurisée, adaptée aux besoins d’expansion de Kasgrunt, tout en optimisant les coûts de communication et en garantissant une haute disponibilité des services essentiels.**