Gestion des risques : Les 4 stratégies de réponse

🎯 **Objectif de cet aide-mémoire**
Comprendre les 4 stratégies de réponse aux risques (Éviter, Transférer, Atténuer, Accepter) et savoir les appliquer dans un projet IT.

📊 **Processus de gestion des risques**

1. **Identifier**
   Lister tous les risques potentiels qui pourraient impacter le projet (brainstorming, retour d'expérience, analyse des dépendances)
2. **Analyser**
   Pour chaque risque, évaluer sa Probabilité (Faible/Moyenne/Élevée) et son Impact (Faible/Moyen/Élevé). Calculer la Criticité (Probabilité × Impact)
3. **Planifier les réponses**
   Pour chaque risque significatif, choisir une stratégie de réponse (Éviter, Transférer, Atténuer, Accepter) et définir un plan d'action concret
4. **Surveiller**
   Suivre l'évolution des risques tout au long du projet. Réévaluer régulièrement la probabilité et l'impact. Activer les plans de réponse si nécessaire

🛡️ **Les 4 stratégies de réponse aux risques**

1. ÉVITER (Eliminate)

Principe

Éliminer complètement le risque en modifiant le plan du projet pour qu'il ne puisse plus se produire.

Quand utiliser cette stratégie ?

• Le risque a un impact très élevé (catastrophique)

• Il est possible de modifier le projet pour éliminer le risque

• Le coût de l'évitement est acceptable

Exemples d'actions pour éviter un risque :

• Changer de technologie ou de fournisseur

• Simplifier le périmètre du projet

• Ajouter des ressources pour réduire les dépendances critiques

Risque IT	Comment ÉVITER ce risque
Incompatibilité entre le nouveau logiciel et l'ancien matériel	Remplacer tout le matériel par du matériel récent compatible AVANT d'installer le nouveau logiciel. Coût élevé, mais risque éliminé.
Perte de données lors d'une migration de serveur	Faire une sauvegarde complète PUIS une copie de la sauvegarde sur un support externe AVANT la migration. Conserver les anciennes données jusqu'à validation complète.
Dépendance critique sur un seul consultant externe	Former 2 personnes internes sur les compétences du consultant dès le début du projet, pour ne plus dépendre uniquement de lui.
Délai trop court pour livrer un projet complexe	Négocier avec le client pour allonger le délai dès le départ, ou réduire le périmètre initial. Éviter d'accepter un projet qu'on sait infaisable.

2. TRANSFÉRER (Transfer)

Principe

Transférer le risque (et ses conséquences) à une tierce partie. Le risque existe toujours, mais c'est quelqu'un d'autre qui en assume la responsabilité financière ou opérationnelle.

Quand utiliser cette stratégie ?

• Le risque a un impact financier important

• Il existe une tierce partie qui peut assumer le risque

• Le coût du transfert (assurance, garantie) est inférieur au coût du risque

Moyens de transférer un risque :

• Souscrire une assurance

• Exiger une garantie fournisseur

• Sous-traiter une partie du projet

• Clauses contractuelles (pénalités de retard)

Risque IT	Comment TRANSFÉRER ce risque
Panne matérielle du serveur pendant la garantie	Acheter une extension de garantie "remplacement J+1" auprès du fournisseur. Si le serveur tombe en panne, c'est le fournisseur qui assume le coût et le délai de remplacement.
Retard de livraison du matériel par le fournisseur	Insérer une clause de pénalité de retard dans le contrat fournisseur (ex : -500 €/jour de retard). Le fournisseur est incité à livrer à temps, et si retard, il compense financièrement.

Risque IT	Comment TRANSFÉRER ce risque
Cyberattaque ou perte de données	Souscrire une assurance cyber-risque qui couvre les pertes financières et les coûts de remédiation en cas d'incident de sécurité.
Complexité technique d'une migration	Sous-traiter la migration à un prestataire spécialisé. Si la migration échoue ou prend du retard, c'est le prestataire qui assume les coûts supplémentaires (selon le contrat).

3. ATTÉNUER (Mitigate)

Principe

Réduire la probabilité d'occurrence du risque et/ou réduire son impact s'il se produit. C'est la stratégie la plus courante en gestion de projet.

Quand utiliser cette stratégie ?

• Le risque ne peut pas être évité ou transféré

• Le risque est trop fréquent ou trop probable

• Des actions concrètes peuvent réduire la probabilité ou l'impact

Actions pour atténuer un risque :

• Ajouter des contrôles ou des tests

• Prévoir des marges (budget, délai)

• Former l'équipe

• Multiplier les sources ou les fournisseurs

Risque IT	Comment ATTÉNUER ce risque
Retard de livraison du matériel	**Réduire la probabilité :** Commander 2 semaines en avance. Identifier un fournisseur alternatif. **Réduire l'impact :** Prévoir 3 jours de marge dans le planning pour absorber un léger retard.
Bugs dans le code déployé en production	**Réduire la probabilité :** Mettre en place des tests automatisés (unitaires, intégration). Faire des revues de code. **Réduire l'impact :** Prévoir un plan de rollback (retour arrière) en cas de bug critique.
Départ d'un membre clé de l'équipe	**Réduire la probabilité :** Créer un bon climat de travail, proposer des formations. **Réduire l'impact :** Documenter le travail de chacun, faire du binômage pour que plusieurs personnes connaissent chaque partie du projet.

Risque IT	Comment ATTÉNUER ce risque
Incompatibilité technique entre deux systèmes	**Réduire la probabilité :** Faire un POC (Proof of Concept) ou un test d'intégration AVANT de commencer le projet. **Réduire l'impact :** Prévoir un budget de contingence (10% du budget total) pour des ajustements imprévus.
Résistance au changement des utilisateurs	**Réduire la probabilité :** Impliquer les utilisateurs dès le début du projet (ateliers, demos régulières). Communiquer sur les bénéfices. **Réduire l'impact :** Prévoir une période d'accompagnement post-déploiement (hotline, documentation, FAQ).

4. ACCEPTER (Accept)

Principe

Reconnaître l'existence du risque et décider de ne rien faire de manière proactive. On accepte les conséquences si le risque se matérialise. Deux variantes : acceptation active (avec plan de contingence) ou passive (sans plan).

Quand utiliser cette stratégie ?

• Le risque a un impact faible ou négligeable

• La probabilité est très faible (risque improbable)

• Le coût de l'atténuation est supérieur au coût du risque

• Aucune action rentable n'est possible

Deux types d'acceptation :

Acceptation active : On prévoit un plan de contingence (budget de réserve, plan B) au cas où le risque se produit.

Acceptation passive : On ne fait rien. On gérera le problème s'il arrive, mais on ne prévoit rien à l'avance.

Risque IT	Comment ACCEPTER ce risque
Légère hausse du prix d'une licence logicielle	**Acceptation passive :** L'impact financier est minime (+200 € sur un projet de 50 000 €). On accepte de payer la différence si ça arrive, sans prévoir de budget supplémentaire.
Absence d'un membre de l'équipe pendant 2-3 jours	**Acceptation passive :** Probabilité moyenne (maladie, congé), mais impact faible (les autres membres peuvent compenser 2-3 jours). On ne fait rien de spécifique.
Panne d'un serveur non critique (serveur de test)	**Acceptation active :** Probabilité faible, impact moyen (ralentissement des tests). On accepte le risque, mais on prévoit un budget de 2 000 € pour acheter une pièce de rechange en urgence si ça arrive.

Risque IT	Comment ACCEPTER ce risque
Changement de réglementation pendant le projet	**Acceptation active :** Probabilité faible, mais impact potentiellement élevé. On accepte le risque et on prévoit 5% du budget en réserve pour adapter le projet si une nouvelle loi est votée.

🧭 **Comment choisir la bonne stratégie ?**

Arbre de décision

Processus de décision

1. Le risque a-t-il un impact catastrophique (perte de données, arrêt complet du service, dépassement majeur de budget) ?

→ Oui : Privilégier **ÉVITER** ou **TRANSFÉRER**

→ Non : Passer à la question 2

2. Peut-on éliminer complètement le risque en modifiant le plan du projet ?

→ Oui et c'est acceptable : **ÉVITER**

→ Non : Passer à la question 3

3. Existe-t-il une tierce partie qui peut assumer le risque (assurance, garantie, sous-traitant) ?

→ Oui et le coût est raisonnable : **TRANSFÉRER**

→ Non : Passer à la question 4

4. Des actions concrètes peuvent-elles réduire significativement la probabilité ou l'impact du risque ?

→ Oui : **ATTÉNUER** (c'est la stratégie par défaut pour la majorité des risques)

→ Non : **ACCEPTER** (le risque est trop faible ou trop coûteux à traiter)

Matrice Probabilité × Impact

Impact \ Probabilité	Faible	Moyenne	Élevée
Élevé	ATTÉNUER ou TRANSFÉRER	ATTÉNUER ou ÉVITER	ÉVITER
Moyen	ACCEPTER (actif)	ATTÉNUER	ATTÉNUER ou ÉVITER
Faible	ACCEPTER (passif)	ACCEPTER (actif)	ATTÉNUER

📋 **Exemple complet : Registre des risques pour un projet VPN**

ID	Risque	Proba	Impact	Criticité	Stratégie	Plan d'action
R01	Incompatibilité VPN avec firewall existant	Moyenne	Élevé	Élevée	**ATTÉNUER**	Faire un POC en semaine 1 pour valider l'interopérabilité. Budget de contingence de 3 000 € pour remplacer le firewall si incompatibilité.
R02	Retard de livraison du serveur VPN	Moyenne	Moyen	Moyenne	**ATTÉNUER**	Commander 2 semaines en avance. Identifier un fournisseur alternatif (LDLC). Prévoir 3 jours de marge dans le planning.
R03	Résistance au changement des utilisateurs	Élevée	Faible	Moyenne	**ATTÉNUER**	Impliquer les utilisateurs dès le début (enquête besoins). Formation en présentiel (2h). Hotline post-déploiement (1 semaine).
R04	Panne du serveur VPN en production	Faible	Élevé	Moyenne	**TRANSFÉRER**	Acheter une extension de garantie "remplacement J+1" (600 €). Le fournisseur assume le risque de panne matérielle.
R05	Cyberattaque pendant la phase de déploiement	Faible	Élevé	Moyenne	**ATTÉNUER**	Déployer un firewall avec règles strictes dès le début. Tests de sécurité (scan vulnérabilités) avant mise en prod. Sauvegarde complète avant déploiement.
R06	Départ du chef de projet en cours de mission	Faible	Moyen	Faible	**ACCEPTER (actif)**	Documentation complète du projet dans GitLab. Un chef de projet adjoint connaît le projet et peut reprendre en cas d'imprévu.
R07	Légère hausse du prix des licences	Moyenne	Faible	Faible	**ACCEPTER (passif)**	Aucun plan spécifique. On paiera la différence si ça arrive (+200 € max sur 15 000 €).

📌 **Synthèse : Les 4 stratégies en un coup d'œil**

Stratégie	Principe	Quand l'utiliser	Exemple d'action
ÉVITER	Éliminer le risque	Impact catastrophique, modification du projet possible	Changer de technologie, simplifier le périmètre, renforcer les ressources
TRANSFÉRER	Faire assumer par un tiers	Impact financier élevé, tiers disponible	Assurance, garantie fournisseur, sous-traitance, clauses contractuelles
ATTÉNUER	Réduire probabilité et/ou impact	Risque fréquent, actions concrètes possibles	Tests, marges, formation, fournisseurs multiples, POC
ACCEPTER	Ne rien faire (actif ou passif)	Impact faible, probabilité faible, coût d'atténuation trop élevé	Budget de réserve (actif) ou aucune action (passif)

✅ **À retenir**

- La stratégie **ATTÉNUER** est la plus courante en gestion de projet IT (70% des risques)
- La stratégie **ÉVITER** est réservée aux risques catastrophiques
- La stratégie **TRANSFÉRER** nécessite un tiers (assureur, fournisseur, sous-traitant)
- La stratégie **ACCEPTER** convient aux risques mineurs ou impossibles à traiter

Un bon registre des risques combine plusieurs stratégies selon la nature de chaque risque.