BEAULIEU Rafael
FALLET Elijah
YAHIA CHERIF Fares
INFI2-FI-B

UVSQ université PARIS-SACLAY
IUT de Vélizy-Rambouillet
CAMPUS DE VÉLIZY-VILLACOUBLAY
CAMPUS DE RAMBOUILLET

SAE3.01

Sommaire

Liste exhaustive des risques

Nous avons listé les différents risques qui pèsent sur notre projet.

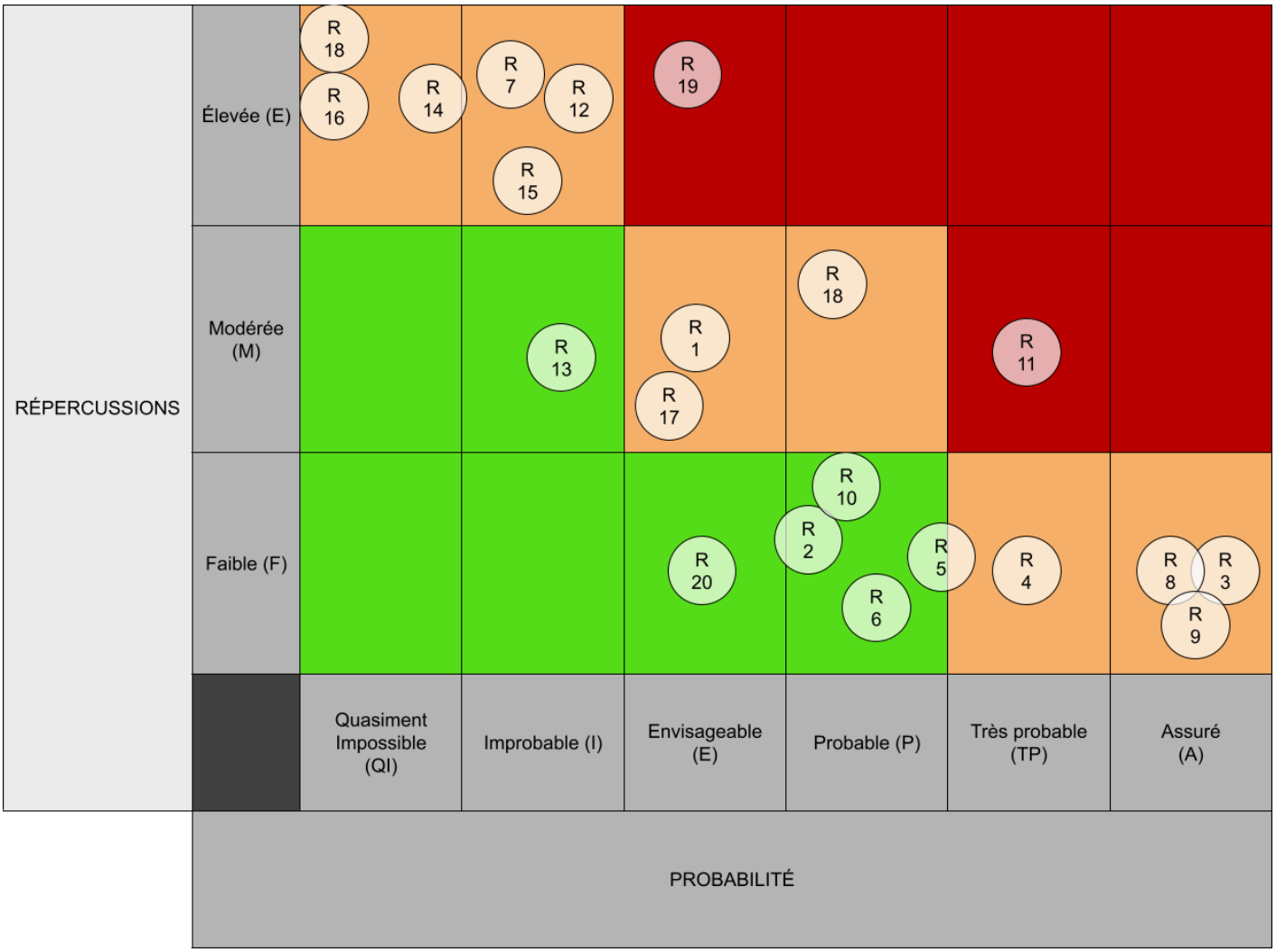
R1	Erreur d'architecture du projet
R2	Base de données mal configurée
R3	Procrastination d'un des membres
R4	Mauvaise répartition du temps
R5	Mauvaise répartition des tâches
R6	Manque de compétences techniques
R7	Défaillance système (panne du disque dur, du processeur, ...)
R8	Conflit au sein de l'équipe
R9	Erreur dans la programmation
R10	Mauvaise communication (mauvaise gestion du git, idées communes mal implémentées, etc...)
R11	Erreur de modélisation
R12	Corruption serveur
R13	Attaque informatique (injection SQL, injection HTML, ...)
R14	Avancé technologique rendant obsolète celles utilisées
R15	Interception des données de connexion
R16	Décès d'un membre
R17	DDoS (Submerger le système de requêtes)
R18	Incident nucléaire
R19	Incendie
R20	Panne de courant

Probabilité d'occurrence des risques

Nous avons classé les différents risques par probabilité d'occurrence.

Risque par probabilité	
Assuré Ce sont les risques qui arriveront assurément au cours du projet	**R3** - Procrastination d'un des membres (faible) **R8** - Conflit au sein de l'équipe (faible) **R9** - Erreur dans la programmation (faible)
Très probable Ce sont les risques ayant de fortes probabilités de survenir plusieurs fois au cours du projet	**R4** - Mauvaise répartition du temps (faible) **R11 -** Erreur de modélisation (modéré)
Probable Ce sont les risque ayant des chance de survenir une ou deux fois au cours du projet	**R2** - Base de données mal configurée (faible) **R5** - Mauvaise répartition des tâches (faible) **R6 -** Manque de compétences techniques (faible) **R10** - Mauvaise communication (faible)
Envisageable Ce sont les risques ayant de peu de chance de survenir au cours du projet mais pouvant être envisagés	**R1** - Erreur d'architecture du projet (modéré) **R17** - DDoS (modéré) **R19** - Incendie (élevé) **R20** - Panne de courant (faible)
Improbable Ce sont les risques n'ayant que très peu de chance de survenir au cours du projet	**R7** - Défaillance système (élevé) **R12** - Corruption de server (élevé) **R13** - Attaque informatique (modéré) **R15** - Interception des données de connexion (élevé)
Quasiment impossible Ce sont les risques ayant une chance infime de survenir au cours du projet. De plus, ces risques ont une incidence élevée sur le projet.	**R14** - Avancé technologique rendant obsolète celles utilisées (élevé) **R16** - Décès d'un des membres (élevé) **R18 -** Incident nucléaire (élevé)

Matrice des risques



Stratégies adoptées

Après avoir identifié les différents risques, nous avons mis en place plusieurs stratégies de gestion :

	Type de stratégie	Détail de la stratégie
R1	réponse conditionnelle	Faire des dessins et schémas en UML au préalable afin de visualiser les rapports entre les différentes parties du programme, ainsi que la base de données et s'assurer du bon fonctionnement de ces liens en planifiant des tests réguliers.
R2	Réponse conditionnelle et évitement	Planifier au mieux les requêtes potentielles afin d'optimiser sa configuration, et effectuer régulièrement des tests sur la base de données.
R3	évitement	Effectuer des mises au points régulières entre les membres
R4	évitement	Prévoir un planning à l'avance en prenant une marge de temps pour finir le projet en faisant par exemple un diagramme de Gantt.
R5	évitement	Mise en place d'outils agiles pour une répartition optimisée afin de garantir la meilleure répartition des tâches.
R6	atténuation	Identifier des solutions alternatives permettant d'atteindre notre but sans utiliser des compétences non acquises.
R7	réponse conditionnelle	trouver un moyen d'avoir accès à du matériel informatique de remplacement
R8	atténuation	Essayer d'identifier la source du conflit et faire de son mieux pour le résoudre par le biais de la discussion, éventuellement avec l'aide d'une personne extérieure, afin de continuer son projet dans la joie et la bonne humeur.
R9	réponse conditionnelle	Identifier la source de l'erreur, et corriger les différents fichiers et lignes de codes en lien avec l'erreur.
R10	atténuation	Afin de réduire le risque, prévoir de nombreuses sessions communes et faire faire les tests de son module par les autres, afin qu'ils puissent fréquemment voir ce qui a été fait et s'assurer que tout le monde s'est compris.
R11	Évitement	Bien définir les objectifs et stratégies à employer avant de s'engager réellement dans le projet en précisant le cahier des charges par exemple.

R12	réponse conditionnelle	Prévoir des sauvegardes régulières, tout le long du projet, afin de pouvoir réinstaurer la dernière sauvegarde dans le cas où le risque se produirait.
R13	Transfert à un tier	Délégation de la sécurité à une entreprise spécialisée pour surveiller le système et agir en conséquence.
R14	atténuation	Faire en sorte de se tenir informé durant le projet, et n'utiliser que des outils fiables et basiques, qui même lors de l'évolution de technologie, ne poserons pas de problèmes
R15	Evitement	Mise en place de différents systèmes sécurisés pour éviter le transfert de données sensibles. Plusieurs tests extensifs de la connexion dans différents contextes seront effectués.
R16	Réponse conditionnel	S'organiser en conséquence, en employant un nouveau membre par exemple.
R17	Transfert à un tier	Mise en place de solutions comme Cloudflare automatisant la gestion du trafic afin d'éviter les attaques réseau.
R18	Réponse conditionnelle	Prioriser la survie des membres du projet.
R19	Atténuation	Mise en place de détecteurs de fumée, portes coupe feu, extincteurs manuels et automatiques dans la limite de notre budget.
R20	Atténuation	Mise en place d'un générateur de secours ou d'un onduleur UPS ainsi que de systèmes permettant la sauvegarde des données en cas de coupure de courant. Répartition du matériel pour assurer la sauvegarde des données en cas de panne.

Conclusion

Au cours des quelques séances où nous avons fait notre projet, nous avons déjà commencé à appliquer certaines des stratégies afin de réagir aux différents risques possibles. Pour commencer, nous avons déjà décidé des objectifs et stratégies à employer au cours du projet afin de réaliser dans les meilleures conditions. Nous avons mis en place un planning ainsi que plusieurs règles et méthodes de travail afin d'encadrer le déroulement du projet. Ces stratégies permettront d'éviter les risques d'erreurs de modélisations **(R11)**, erreurs dans le programme **(R9)**, base de données mal configurée **(R2)**, procrastination d'un membre **(R3)**, conflit au sein de l'équipe **(R8)** ou encore la mauvaise répartition du temps **(R4)**. Nous continuerons d'appliquer les différentes stratégies de gestion des risques durant la suite de notre projet.