

الجمهورية الجزائرية الديمقراطية الشعبية  
République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur  
et de la Recherche Scientifique

Ecole Nationale Supérieure de Management  
Koléa



وزارة التعليم العالي و البحث العلمي

المدرسة الوطنية العليا للمناجنت  
القلبية

## MEMOIRE DE FIN DU CYCLE

En vue de l'obtention d'un master professionnel en

« Entreprenariat et management de projet »

Thème

**Maitrise efficace des risques dans un projet IT**

**Cas : Projet AGB de BEYN (ex : AeBS-Algeria e-Banking services)**

**Élaboré par :**

Mme. Benyoucef Dhouha

**Encadré par :**

Dr. Bedaida Imad Eddine

**Année universitaire**

**2024/2025**

## Résumé

La gestion des risques dans les projets informatiques est un enjeu crucial pour assurer la sécurité des données, la conformité aux réglementations et la confiance des parties prenantes. Cette étude se concentre sur la maîtrise des risques dans le cadre du projet AGB de BEYN (ex-AeBS Algeria e-Banking Services), une fintech algérienne spécialisée dans les solutions numériques bancaires.

Notre recherche vise à analyser l'efficacité des méthodologies de gestion des risques, en particulier l'Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (AMDEC), appliquée au développement d'une plateforme d'e-banking. Pour ce faire, nous avons adopté une approche qualitative basée sur des entretiens semi-directifs avec les acteurs clés du projet (chef de projet, Product Owner, responsable qualité) et une observation directe des processus. Les données recueillies ont été analysées à l'aide du logiciel NVivo et structurées dans une matrice AMDEC.

Les résultats mettent en évidence six catégories de risques majeurs : techniques, sécurité/conformité, organisationnels, financiers, délais et risques externes. Grâce à la mise en place de mesures préventives et correctives, ainsi qu'une amélioration de la gestion des risques modérés et indésirables. Ces actions incluent des tests pilotes renforcés, une infrastructure redondante, l'authentification multi-facteurs et des revues régulières des plannings.

Cette étude confirme l'utilité de l'AMDEC comme outil structurant pour identifier, évaluer et atténuer les risques dans les projets IT, tout en soulignant l'importance d'une approche adaptative combinant rigueur méthodologique et flexibilité opérationnelle. Les recommandations formulées, telles que la formation des équipes et l'intégration de tests automatisés, offrent un cadre actionnable pour les organisations similaires.

Mots clés : AMDEC, gestion des risques, projet IT, e-banking, sécurité informatique, méthodologie Agile.

## **Abstract**

Risk management in IT projects is a crucial issue for ensuring data security, regulatory compliance, and stakeholder trust. This study focuses on risk control within the AGB project at BEYN (formerly AeBS Algeria e-Banking Services), a leading Algerian fintech specializing in digital banking solutions.

Our research aims to analyze the effectiveness of risk management methodologies, particularly the Failure Modes, Effects, and Criticality Analysis (FMECA) applied to the development of an e-banking platform. To achieve this, we adopted a qualitative approach, conducting semi-structured interviews with key project stakeholders (Project Manager, Product Owner, and Quality Manager) and observing the operational processes directly. The collected data was analyzed using NVivo software and structured within an FMECA matrix.

The results highlight six major risk categories: technical, security/compliance, organizational, financial, schedule-related, and external risks. Thanks to the implementation of preventive and corrective measures, as well as improvements in managing moderate and undesirable risks, the project's security has been reinforced. These actions include enhanced pilot testing, redundant infrastructure, multi-factor authentication, and regular project planning reviews.

This study confirms the value of FMECA as a structuring tool for identifying, assessing, and mitigating risks in IT projects, while emphasizing the importance of an adaptive approach that combines methodological rigor and operational flexibility. The formulated recommendations, such as team training and the integration of automated testing, provide a practical framework for similar organizations.

**Keywords:** FMECA, risk management, IT project, e-banking, cybersecurity, Agile methodology.

## ملخص

إدارة المخاطر في المشاريع التقنية تعد عنصرًا أساسيًا لضمان أمن البيانات، والامتثال للتشريعات وكسب ثقة أصحاب المصلحة. تركز هذه الدراسة على التحكم بالمخاطر في إطار مشروع AGB التابع لشركة (BEYN سابقًا AeBS (Algeria e-Banking Services)، وهي شركة فينتك رائدة في الجزائر متخصصة في الحلول المصرفية الرقمية.

تهدف أبحاثنا إلى تحليل فعالية منهجيات إدارة المخاطر لا سيما تحليل أنماط الفشل وتأثيراتها ومؤشر خطورتها (AMDEC)، وتطبيقها في تطوير منصة مصرفية إلكترونية. لتحقيق ذلك اعتمدنا نهجًا نوعيًا يركز على مقابلات شبه منظمة مع الجهات الفاعلة الرئيسية في المشروع (مدير المشروع مالك المنتج ومسؤول الجودة)، بالإضافة إلى المراقبة المباشرة للعمليات التشغيلية. تم تحليل البيانات باستخدام برنامج NVivo وتنسيقها ضمن مصفوفة AMDEC.

أظهرت النتائج ست فئات رئيسية للمخاطر: التقنية الأمان/الامتثال، التنظيمية، المالية، الزمنية، والخارجية. وبفضل تنفيذ الإجراءات الوقائية والتصحيحية إلى جانب تحسين إدارة المخاطر المتوسطة وغير المرغوبة تم تعزيز أمان المشروع. وشملت هذه التدابير اختبارات تجريبية معززة بنية تحتية احتياطية المصادقة متعددة العوامل ومراجعات دورية لخطط التنفيذ.

تؤكد هذه الدراسة على أهمية AMDEC كأداة منهجية لتحديد وتقييم والتخفيف من المخاطر في المشاريع التقنية مع تسليط الضوء على ضرورة تبني نهج تكيفي يجمع بين الصرامة المنهجية والمرونة التشغيلية. توفر التوصيات المطروحة مثل تدريب الفرق ودمج الاختبارات المؤتمتة إطارًا عمليًا يمكن تطبيقه في المؤسسات المشابهة.

الكلمات المفتاحية: AMDEC، إدارة المخاطر المشاريع التقنية الخدمات المصرفية الإلكترونية الأمان السيبراني، منهجية أجایل.

## Remerciement

*Ce travail est le fruit d'un chemin parcouru grâce au soutien précieux de nombreuses personnes. Je tiens avant tout à remercier le Tout-Puissant, qui m'a accordé la santé, la persévérance et la force nécessaire pour mener à bien ce projet, tout en plaçant sur ma route des personnes exceptionnelles.*

*Je souhaite exprimer ma profonde gratitude à **Monsieur Bedaida Imad Eddine**, mon enseignant, pour ses conseils éclairés, sa disponibilité et son accompagnement tout au long de ce mémoire. Ses orientations ont été d'une aide inestimable.*

*Un merci sincère à **Monsieur Mohamed Toubaline**, mon tuteur pour m'avoir offert l'opportunité de réaliser ce travail, pour sa confiance, ses précieuses remarques et son soutien constant dans l'aboutissement de ce projet.*

*Je tiens également à remercier chaleureusement l'ensemble du personnel de **BEYN (ex-AeBS Algeria e-Banking Services)**, qui a contribué à la réussite de ce stage. Leurs partages d'expérience, leurs conseils et leur accueil bienveillant ont grandement enrichi mes recherches et ma compréhension du sujet.*

*Ma gratitude la plus tendre va à **mes parents et à ma famille**, piliers indéfectibles, pour leur amour, leurs encouragements et leurs sacrifices qui m'ont permis d'avancer même dans les moments les plus exigeants.*

## Sommaire

Résumé.....	i
Remerciement .....	iv
Liste des tableaux .....	vi
Liste des figures .....	vii
Liste des abréviations .....	viii
Introduction générale.....	9
CHAPITRE 01 : REVUE DE LITTERATURE ET CADRE CONCEPTUEL .....	11
Section 1 : La revue de la littérature .....	6
Section 2 : Cadre conceptuel de l'étude .....	15
CHAPITRE 02 : METHODOLOGIE DE LA RECHERCHE ET CONTEXTE ORGANISATIONNE .....	11
Section 1 : Méthodologie de la recherche .....	45
Section 2 : Contexte organisationnel .....	54
CHAPITRE 03 : RESULTATS ET DISCUSSION.....	11
Section 1 : résultats de l'étude qualitative.....	62
Section 2 : Discussion .....	72
CONCLUSION GÉNÉRALE.....	11
LISTE BIBLIOGRAPHIQUE .....	11
ANNEXES .....	11

## Liste des tableaux

<b>Tableau 1:</b> Tableau des entretiens .....	49
<b>Tableau 2:</b> Scores d'évaluation de la gravité .....	51
<b>Tableau 3:</b> Scores d'évaluation de la fréquence .....	52
<b>Tableau 4:</b> Scores d'évaluation de la détection .....	52
<b>Tableau 5:</b> Échelle de priorité.....	68
<b>Tableau 6:</b> Classification de l'acceptabilité des risques .....	70
<b>Tableau 7:</b> analyse comparative des criticités. ....	71

## Liste des figures

<b>Figure 1:</b> Processus général de management de projets .....	17
<b>Figure 2:</b> Processus général de management des risques .....	26
<b>Figure 3:</b> organigramme de l'entreprise.....	56
<b>Figure 4:</b> nuage de mots d'axe 01 gestion de projet .....	63
<b>Figure 5:</b> nuage de mots d'axe 02 les Approches classiques de gestion des risques .....	64
<b>Figure 6:</b> nuage de mots d'axe 03 sur les Approches innovantes et Amélioration continue .....	65

## Liste des abréviations

<b>AGB</b>	Algerian Gulf Bank
<b>AMDEC</b>	Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité
<b>BEYN</b>	Beyn (ex-AeBS Algeria e-Banking Services)
<b>BU</b>	Business Unit
<b>DSP2</b>	Directive sur les Services de Paiement (version 2)
<b>FMECA</b>	Failure Mode, Effects, and Criticality Analysis (équivalent anglais de l'AMDEC)
<b>ISO</b>	International Organization for Standardization
<b>IT</b>	Technologies de l'Information (Information Technology)
<b>KM</b>	Knowledge Management (Gestion des Connaissances)
<b>NIST</b>	National Institute of Standards and Technology
<b>NVivo</b>	Logiciel d'analyse qualitative de données
<b>PMBOK</b>	Project Management Body of Knowledge
<b>PMI</b>	Project Management Institute
<b>RBS</b>	Risk Breakdown Structure
<b>RMF</b>	Risk Management Framework
<b>ROE</b>	Return on Equity (Rendement des Capitaux Propres)
<b>SaaS</b>	Software as a Service
<b>SWOT</b>	Strengths, Weaknesses, Opportunities, Threats (Analyse FFOM en français)
<b>VA</b>	Valeur Ajoutée
<b>VaR</b>	Value at Risk (Valeur à Risque)

# **INTRODUCTION GÉNÉRALE**

Dans un environnement financier en constante évolution technologique, les institutions bancaires se trouvent à la croisée des chemins entre tradition et innovation. Face à la numérisation rapide du secteur bancaire, la Banque AGB (Algerian Gulf Bank) a lancé une initiative stratégique pour actualiser ses services numériques, améliorer sa relation avec les clients et offrir une expérience utilisateur avant-gardiste à tous ses clients, qu'ils soient particuliers ou entreprises. Reconnaisant les transformations majeures des pratiques bancaires, AGB a identifié l'impératif de réviser son canal numérique par le biais d'une révision intégrale de son système de banque en ligne.

Dans le but d'atteindre cet objectif, la banque a lancé un projet majeur visant à déployer une solution de Digital Banking de nouvelle génération, conçue pour succéder à l'actuelle plateforme e-banking en service. Cette initiative vise à se conformer aux normes internationales en termes de digitalisation, tout en considérant les particularités du marché algérien et les exigences de sa clientèle. Le projet a été présenté dans le cadre d'une consultation restreinte, visant des fournisseurs reconnus pour leur compétence en matière de banque numérique et de sécurité bancaire. C'est dans ce contexte que l'entreprise BEYN a été choisie pour la création de la nouvelle plateforme d'e-banking d'AGB. La proposition de BEYN s'est démarquée grâce à sa connaissance approfondie des technologies bancaires, l'étendue des fonctionnalités de sa solution et son aptitude à personnaliser le produit en fonction des exigences métiers spécifiques d'AGB.

Cette transformation numérique s'inscrit dans un contexte plus large où la digitalisation des services financiers redéfinit profondément le paysage bancaire mondial. Cependant, cette évolution s'accompagne inévitablement de nouveaux défis, particulièrement en matière de gestion des risques informatiques. La sécurité des données, la conformité réglementaire et la continuité des services deviennent des préoccupations majeures pour les institutions financières comme AGB.

L'ampleur de ce projet de modernisation soulève des questions fondamentales sur les méthodologies à adopter pour garantir son succès tout en maîtrisant les risques inhérents. Dans ce cadre, les approches agiles émergent comme une alternative prometteuse aux méthodes traditionnelles de gestion de projet.

Notre étude se propose d'explorer **comment la méthode agile peut contribuer à une maîtrise plus efficace des risques dans les projets IT ?**

Cette problématique centrale se décline en plusieurs axes d'investigation :

Quelles sont les principales méthodes utilisées en gestion des risques ?

Comment évaluer l'efficacité comparée des approches traditionnelles et émergentes ?

Quels défis spécifiques se posent lors de la mise en œuvre des méthodes de gestion des risques dans le contexte bancaire algérien ?

Et enfin, comment concevoir un cadre méthodologique suffisamment adaptable pour améliorer la gestion des risques dans un environnement aussi dynamique que celui des services financiers numériques ?

À travers cette étude, nous explorons l'impact des différentes approches de gestion des risques, en mettant un accent particulier sur l'agilité et ses bénéfices en matière de réduction des incertitudes dans les projets IT.

## **2. Méthodologie**

Pour répondre à cette problématique, nous avons adopté une méthodologie qualitative, combinant des entretiens semi-directifs avec les acteurs clés du projet AGB, une analyse documentaire des référentiels normatifs (ISO 31000, PMBOK), et l'application de l'AMDEC pour hiérarchiser les risques. En complément, l'outil NVivo a été mobilisé pour structurer et analyser les données recueillies.

## **3. Choix de l'organisme d'accueil**

Le choix de BEYN comme organisme d'accueil s'inscrit dans une démarche d'étude de cas pertinente. Fintech algérienne spécialisée dans les solutions numériques bancaires, BEYN représente un acteur clé de la transformation digitale du secteur financier. Le projet AGB, qui consiste en la mise en place d'une nouvelle plateforme d'e-banking, offre un terrain d'analyse idéal pour observer la gestion des risques dans un environnement complexe et fortement réglementé.

## **4. Intérêt de l'étude**

Cette recherche présente un double intérêt. D'un point de vue théorique, elle contribue à enrichir la littérature sur la gestion des risques dans les projets IT, notamment dans le contexte des fintechs. Sur le plan pratique, elle propose des recommandations stratégiques pour optimiser la gestion des risques au sein de BEYN et d'autres organisations similaires. L'étude vise également à identifier les bonnes pratiques des méthodologies de projet (Agile, Waterfall, Hybride) et à améliorer les outils existants, tels que l'AMDEC et les matrices de criticité.

## **5. Annonce du plan**

Afin de structurer cette recherche, nous avons organisé l'analyse en trois chapitres.

Le premier chapitre propose une revue de littérature sur les méthodologies de gestion de projet et les outils d'analyse des risques.

Le deuxième chapitre présente la méthodologie adoptée, le contexte organisationnel de BEYN et l'étude détaillée du projet AGB.

Enfin, le troisième chapitre expose les résultats obtenus, mettant en lumière les vulnérabilités identifiées et les mesures correctives envisagées, Nous concluons notre étude sur les résultats obtenus et les éventuelles perspectives d'évolution.

**CHAPITRE 01 : REVUE DE  
LITTERATURE ET CADRE  
CONCEPTUEL**

L'accélération de la transformation numérique a profondément redéfini l'écosystème des risques pour les entreprises. À l'ère où les systèmes d'information constituent l'épine dorsale des opérations commerciales, la cybersécurité et la maîtrise des risques digitaux revêtent une importance stratégique incontournable. Cette étude examine les principes théoriques et les méthodologies opérationnelles de la gestion des risques appliqués aux projets informatiques, en se focalisant sur le domaine sensible de la banque en ligne, où les impératifs de sécurité atteignent un niveau de criticité élevé.

## **Section 1 : La revue de la littérature**

Ce chapitre explore les différentes facettes de la cybersécurité et de la gestion des risques numériques dans un projet IT. Nous analyserons les travaux de recherche antérieurs sur ces sujets et mettrons en lumière les stratégies permettant d'intégrer efficacement la gestion des risques dans la transformation digitale des entreprises. En outre, nous examinerons les fondamentaux de la gestion des risques, notamment l'approche AMDEC (Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité) et son application dans le contexte numérique.

L'ensemble de ces éléments constitue une base essentielle pour assurer la robustesse des plateformes digitales face aux menaces et garantir leur fonctionnement optimal dans un projet IT.

### **1. Le management des risques**

L'objectif principal de la gestion des risques est d'assurer une performance optimale des projets tout en réduisant les incertitudes. L'article de (Claudiu, 2007), PhD, maître de conférences à l'Université de Craiova, analyse les multiples dimensions de la gestion des risques dans les projets en mettant l'accent sur l'identification, l'analyse, la minimisation et la planification des contingences. Son objectif est de proposer des stratégies adaptées pour équilibrer efficacement les contraintes des projets, telles que le temps, les ressources, les coûts et l'étendue des tâches, tout en gérant les incertitudes inhérentes. L'approche méthodologique repose sur une analyse descriptive et théorique, intégrant des outils comme des listes de contrôle, des techniques de brainstorming, et des matrices qualitatives classant les risques selon leur probabilité et leur impact. L'article détaille également des stratégies de gestion telles que l'acceptation, le transfert, l'évitement et l'atténuation des risques. Bien qu'il offre un cadre structuré et des recommandations utiles, son manque d'études de cas empiriques limite son applicabilité pratique et certaines propositions restent générales. L'article souligne que la gestion des risques est indispensable pour réduire les incertitudes à

un niveau acceptable et garantir un alignement équilibré entre les objectifs et les contraintes des projets, tout en insistant sur l'importance de la flexibilité et des plans de contingence pour faire face aux imprévus

Dans leur article « Le management des risques : cadre théorique », publié dans l'*International Journal of Accounting, Finance, Auditing, Management and Economics*, (ALAOUI & DHIBA, 2022) fournissent un cadre théorique complet pour la gestion des risques. Les auteurs explorent systématiquement les fondements conceptuels de la gestion des risques, retraçant son évolution d'une approche réactive, basée sur l'assurance, à une stratégie organisationnelle proactive et intégrée. Ils soulignent la double nature du risque, qui englobe à la fois les menaces et les opportunités, et mettent en évidence son impact sur la résilience et les performances de l'organisation. L'étude classe les risques en trois catégories : financiers, opérationnels et stratégiques, conformément aux normes ISO 31000. Elle critique les outils de mesure traditionnels tels que la valeur à risque (VaR), tout en préconisant des méthodologies dynamiques et sensibles au contexte. L'analyse détaillée du processus de gestion des risques, qui met en avant la communication, l'adaptation au contexte et le suivi itératif, constitue une contribution essentielle. Cependant, l'accent mis sur les modèles théoriques peut limiter l'applicabilité immédiate de l'article aux défis spécifiques du secteur. Ce travail offrant une définition holistique de la gestion des risques et en validant le besoin de cadres adaptatifs dans les contextes de projet, faisant le lien entre la rigueur théorique et la pertinence managériale.

(Rodrigues-da-Silva & Crispim, 2014) Présentent un cadre complet pour aligner les pratiques de gestion des risques sur la maturité organisationnelle, la complexité du projet et les phases du cycle de vie, répondant ainsi au besoin d'outils de MPR adaptables. Leur examen systématique de 56 articles (1995-2013) a permis d'identifier 115 pratiques de gestion des risques, qui ont ensuite été affinées en 60 techniques validées empiriquement et organisées en six étapes : identification, analyse, planification de l'atténuation, contrôle, rapports et soutien. Leur cadre se distingue par l'intégration de la maturité organisationnelle et de la complexité du projet, reconnaissant que des facteurs tels qu'une culture du risque proactive et la diversité des parties prenantes ont un impact significatif sur l'efficacité de la gestion des risques. L'une des principales conclusions de l'étude est la partialité sectorielle de la littérature existante : 62 % des pratiques étudiées proviennent des secteurs des technologies de l'information et de la construction, qui sont très réglementés et complexes. L'étude souligne que les techniques avancées telles que la simulation de Monte Carlo et la

gestion de la valeur acquise sont plus efficaces pour les organisations matures qui gèrent des projets complexes, tandis que les outils plus simples tels que les registres de risques et les listes de contrôle sont suffisants pour les environnements moins exigeants. Toutefois, le fait qu'elle s'appuie sur des données d'enquête autodéclarées et des études de cas préliminaires suggère qu'il est nécessaire de procéder à d'autres tests empiriques dans différents secteurs d'activité.

## **2. Maîtrise des risques dans le secteur E-banking**

La gestion des risques est un élément clé pour assurer le succès des projets, en particulier dans des domaines complexes tels que les services informatiques. (Benoit, Sylvie, Patry, & Rivard, 1998) Fournissent un cadre de base pour la gestion des risques dans l'externalisation des technologies de l'information, fondé sur la théorie de l'agence et l'économie des coûts de transaction. Leurs études de cas de deux grands projets d'externalisation dans le secteur de l'assurance - une mise à niveau du système pour le passage à l'an 2000 et un partenariat de développement d'applications - aident à définir l'exposition au risque sur la base de la probabilité et de la perte potentielle.

Leur cadre met en évidence sept risques clés, tels que le verrouillage, la dégradation du service et les modifications coûteuses du contrat, chacun étant lié à des facteurs tels que l'opportunisme du fournisseur et l'incertitude technologique. Pour atténuer ces risques, ils proposent des modèles de contrats stratégiques, notamment des pénalités basées sur les performances, des contrats échelonnés et des achats multiples, afin de prévenir les résultats négatifs (stratégie de prudence) ou d'en réduire l'impact (stratégie de tolérance).

Bien que leur travail s'applique principalement à l'externalisation traditionnelle des technologies de l'information, l'accent qu'ils mettent sur l'évaluation dynamique des risques correspond bien à la banque en ligne moderne, d'autant plus que 42 % des risques d'externalisation proviennent des interdépendances et des défis de mesure - des préoccupations critiques dans la fintech, où les intégrations API et le suivi des transactions en temps réel ajoutent à la complexité.

(KHELIFA & DERRADJI, 2016), au début des années 2000, analysent la double nature de la banque électronique, soulignant ses gains d'efficacité ainsi que l'amplification des risques traditionnels (opérationnels, de réputation) et des nouvelles vulnérabilités (par exemple, l'arbitrage réglementaire transfrontalier, la cybercriminalité). S'appuyant sur des études de

cas internationales menées en Scandinavie, aux États-Unis et en Asie, les auteurs identifient quatre catégories de risques critiques :

(2) les risques juridiques, notamment le non-respect des lois sur la protection des données et le blanchiment d'argent facilité par l'anonymat des clients ;

- les risques juridiques, notamment le non-respect des lois sur la protection des données et le blanchiment d'argent facilité par l'anonymat des clients ;

(3) les risques opérationnels, en particulier les menaces de cybersécurité qui pèsent sur l'intégrité des systèmes ; et

(4) les risques de réputation découlant des interruptions de service ou des atteintes à la sécurité, début des années 2000, pp. 404-406). L'étude souligne que si la banque en ligne élargit l'accès au marché (par exemple, 75 % des banques scandinaves offraient des services en ligne en 2001), sa nature sans frontières complique la surveillance, ce qui nécessite une harmonisation internationale de la réglementation — un défi souligné par les principes du Comité de Bâle de 2001 pour la gestion des risques liés à la banque électronique (p. 406).

(Achibane & Allam, 2019) Explorent comment les banques marocaines équilibrent la conformité réglementaire et la gestion du risque opérationnel dans le cadre de Bâle III. Leur étude, qui s'étend sur une décennie (2006-2017), révèle que les banques ont maintenu de solides ratios de solvabilité (13,9 % contre 12 % au minimum) tout en réussissant à réduire les prêts non performants de 11 % à 8 %, ce qui témoigne d'un contrôle efficace des risques.

Trois constats essentiels se dégagent :

1. La conformité réglementaire améliore la stabilité systémique (par exemple, la couverture des liquidités à 152 %) mais limite la rentabilité à court terme, comme le montre la baisse du rendement des capitaux propres (ROE) de 20,6 % à 9,5 %.

2. Les outils opérationnels tels que l'évaluation des clients et les contrôles internes aident à gérer le risque de crédit, mais les banques qui s'appuient trop sur des références externes (comme les scores BDFI) peuvent mal évaluer les vulnérabilités spécifiques au secteur.

3. Les tensions macroéconomiques et institutionnelles se manifestent lorsque les dispositions de Bâle sur l'aversion au risque (par exemple, la couverture totale des prêts compromis) se heurtent à la nécessité d'une innovation financière agile.

Bien que l'étude soit centrée sur la banque traditionnelle, sa critique de la procyclicité de Bâle s'aligne sur les défis de la banque en ligne, où la croissance numérique rapide va souvent plus vite que l'évolution de la réglementation. L'une des limites notables de l'étude est l'absence de risques liés à la cybersécurité, cruciale pour la finance numérique. Cependant, l'accent mis sur les tampons de capital dynamiques (tels que les coussins contracycliques) offre des perspectives précieuses qui sont directement liées aux stratégies de risque adaptatives dans la banque numérique.

(AMEDZRO St-HILAIRE, 2014) Étudie l'impact des mécanismes de contrôle des risques sur la performance des projets des entreprises non financières, en analysant 206 entreprises sur 1 438 années d'observation. En utilisant des modèles GMM dynamiques, l'étude met en évidence l'influence des structures de risque (comme l'indépendance du conseil d'administration et des comités d'audit) et des types de propriété sur les mesures financières clés (ROA, ROIC, Q de Tobin).

Cette étude valide les leviers de gouvernance en montrant qu'une forte surveillance du conseil d'administration et des audits indépendants réduisent les risques opérationnels, des idées qui s'appliquent aux réglementations bancaires électroniques comme la conformité à la DSP2. En outre, l'impact des investisseurs étrangers s'aligne sur les stratégies de partage des risques des banques en ligne transfrontalières.

Bien qu'elle se concentre sur les secteurs non financiers, l'accent mis par l'étude sur la gouvernance adaptative résonne avec le besoin de cadres de risque flexibles de la banque en ligne, en particulier pour faire face aux risques de cybersécurité - une lacune importante par rapport aux modèles de risque traditionnels.

Bien que l'étude soit antérieure à l'essor de la banque numérique, ses conclusions sur la dynamique de l'actionnariat et la structure des conseils d'administration sont riches d'enseignements. Alors que la banque en ligne est confrontée à des défis réglementaires et technologiques.

### **3. Les défis de maîtrise des risques**

( Le Coze, et al., 2020), explorent les nouveaux défis de l'analyse des risques dans les contextes industriels, en soulignant comment les transitions numériques, environnementales et systémiques révèlent les limites des modèles traditionnels. Ils critiquent sa subjectivité, illustrée par des échecs tels que Fukushima et Lubrizol, où des risques négligés - comme la sous-estimation de la hauteur des tsunamis et les dépendances cyber-physiques - ont entraîné

de graves conséquences. Leur étude identifie les principales contraintes, notamment le dimensionnement défectueux des scénarios, les biais de probabilité, le décalage entre les modèles de risque théoriques et les applications dans le monde réel, et la surveillance des menaces émergentes telles que les cyberattaques et les effets en cascade. Pour combler ces lacunes, ils préconisent l'intégration d'outils numériques, tels que les modèles de l'arbre d'attaque et du nœud papillon, afin d'améliorer l'évaluation dynamique des risques. En outre, ils soulignent l'importance de cadres tels que Natech, qui tiennent compte de l'intersection des risques naturels et technologiques, ainsi que des évaluations de l'impact sur l'environnement pour améliorer la résilience. Leurs conclusions mettent en évidence la nécessité d'adopter des approches adaptatives et interdisciplinaires, qui s'inscrivent dans la lignée des défis posés par la banque en ligne, où les menaces de cybersécurité et les risques systémiques exigent une flexibilité similaire. En fin de compte, leur travail contribue à des discussions plus larges sur l'équilibre entre la précision technique et la responsabilité socio-environnementale.

(EMS, 2013), explore la gestion des risques numériques dans les administrations territoriales françaises, mettant en évidence des lacunes critiques en matière de cybersécurité malgré l'utilisation généralisée des outils de gouvernance électronique. Son étude met l'accent sur la difficulté d'aligner les mesures de protection techniques sur la culture organisationnelle, une préoccupation également pertinente dans le domaine de la banque en ligne, où la numérisation rapide dépasse souvent les connaissances des parties prenantes en matière de risques. Par contre ( RAÏS , 2012) examine les stratégies de risque dans les entreprises non financières, en soulignant comment le secteur, la taille et la liquidité influencent la sophistication de la gestion des risques. Il est intéressant de noter que les entreprises de taille moyenne ont tendance à privilégier l'assurance interne au transfert de risque externe (comme les produits dérivés), un paradoxe auquel les fintechs sont confrontées lorsqu'elles cherchent à concilier agilité et résilience. Pour le e-banking, cela renforce la nécessité d'intégrer des modèles de risque quantitatifs à des stratégies qualitatives, telles que la formation des employés et les partenariats intersectoriels, afin de construire un écosystème financier plus adaptable et plus résistant.

D'autre part, ( GOURINE, 2013) adopte une approche différente, préconisant des modèles de partage des risques transorganisationnels inspirés des traditions de solidarité maghrébines (twizas), mettant l'accent sur l'hospitalité culturelle en tant qu'outil d'atténuation proactive des risques. Ses idées s'alignent sur la dépendance croissante des services bancaires en ligne

à l'égard des cadres de collaboration, tels que la prévention de la fraude transfrontalière. Ensemble, ces études mettent en évidence la tension permanente entre les outils techniques de gestion des risques (par exemple, les produits dérivés, les protocoles de cybersécurité) et les facteurs humains/organisationnels (par exemple, la culture, la communication).

(Mercier-Laurent, 2016), explore le rôle vital de la gestion des connaissances (KM) dans le contrôle des risques, en soulignant l'importance d'intégrer une expertise multidisciplinaire pour anticiper et atténuer les risques modernes. L'étude classe les risques en menaces industrielles, organisationnelles, technologiques et émergentes (comme la cybersécurité et la biotechnologie), en soulignant comment la mondialisation et la numérisation exacerbent ces défis. L'une des principales conclusions est que de nombreux risques systémiques découlent de défaillances humaines et organisationnelles, telles qu'une mauvaise maintenance, des biais cognitifs et des lacunes en matière de gestion, comme en témoignent des catastrophes telles que l'explosion de Buncefield en 2005, où les leçons du passé n'ont pas été prises en compte. Mercier-Laurent critique les limites des approches réactives du risque et préconise plutôt des stratégies proactives telles que la maintenance préventive, les évaluations probabilistes de la sécurité (EPS) et les outils de gestion des connaissances (tels que les réseaux bayésiens et l'apprentissage profond) pour prédire les risques et sauvegarder l'expertise institutionnelle. Malgré ces progrès, l'adoption de la gestion des connaissances se heurte à des obstacles, notamment les priorités à court terme des entreprises et la sous-évaluation des actifs incorporels. Ce cadre est directement lié aux risques liés à la banque en ligne, où les lacunes en matière de connaissances sur les protocoles de cybersécurité et la conformité réglementaire constituent des menaces similaires dans un contexte d'évolution technologique rapide. En fin de compte, l'accent mis par l'étude sur la gestion des connaissances en tant qu'outil de résilience aux risques offre une perspective précieuse pour l'identification des vulnérabilités spécifiques au secteur et l'élaboration de solutions fondées sur les connaissances dans le domaine de la finance numérique.

(AFNOR, Gestion des risques projet IT , 2003), propose une approche structurée de la gestion des risques liés aux projets informatiques, qui comprend l'identification, l'évaluation et l'atténuation. L'étude souligne la nature itérative du contrôle des risques, en particulier dans les environnements informatiques où les risques techniques, humains et juridiques - tels que la pénurie de ressources, les changements réglementaires et l'obsolescence technologique - exigent des stratégies adaptatives. L'un des principaux défis identifiés est la difficulté de hiérarchiser les risques de manière dynamique, car les matrices de criticité - qui

équilibrent la probabilité et l'impact - échouent souvent en raison de biais cognitifs ou de résistances organisationnelles, telles que la sous-estimation des conflits entre les parties prenantes. Une étude de cas sur les systèmes d'archivage électronique met en évidence ces problèmes, en montrant comment les retards des fournisseurs et l'évolution de la législation peuvent intensifier les risques malgré des mesures proactives. Si le cadre de l'AFNOR comprend des méthodologies précieuses telles que les techniques Delphi et les analyses post-mortem, il révèle également une lacune critique : sa dépendance à l'égard de la documentation statique, qui peut entraver la réactivité en temps réel dans des paysages informatiques en évolution rapide.

#### **4. Analyse critique**

La recherche présente la gestion des risques comme une discipline dynamique, coincée entre des cadres établis et des complexités émergentes. Alors que des études fondamentales comme celle (Claudiu, 2007) fournissent des structures essentielles pour l'identification et l'atténuation des risques, et qu' (ALAOUI & DHIBA, 2022) les développent en une approche stratégique alignée sur les normes ISO, leurs modèles théoriques sont confrontés à des défis concrets. Une tension frappante émerge entre les méthodologies prescrites et la mise en œuvre réelle - où les outils qualitatifs tels que les matrices de risques s'avèrent insuffisants pour les projets complexes sans maturité organisationnelle (Rodrigues-da-Silva & Crispim, 2014) Ce décalage est aggravé par un biais sectoriel flagrant, la plupart des pratiques étudiées étant dérivées des technologies de l'information et de la construction, laissant les autres industries sans solutions adaptées.

L'évolution de la gestion des risques liés à la banque en ligne révèle un bras de fer permanent entre l'innovation et le contrôle. Alors que les premiers cadres issus de l'externalisation des technologies de l'information (Benoit, Sylvie, Patry, & Rivard, 1998) identifiaient des défis intemporels tels que le verrouillage des fournisseurs, les écosystèmes bancaires et DeFi d'aujourd'hui, pilotés par des API, ont considérablement élargi le paysage des risques. Les chercheurs ont progressivement découvert des couches plus profondes de vulnérabilité - des lacunes réglementaires transfrontalières (KHELIFA & DERRADJI, 2016) aux effets étouffants sur l'innovation d'une conformité rigoureuse (Achibane & Allam, 2019). Ce qui émerge est un paradoxe : les réglementations mêmes conçues pour assurer la stabilité (comme les coussins de capital de Bâle III) peuvent involontairement entraver l'agilité nécessaire pour faire face aux menaces émergentes telles que la fraude induite par l'IA. Même les études sur la gouvernance d'autres secteurs (AMEDZRO St-HILAIRE, 2014) bien

qu'utiles, ne parviennent pas à saisir pleinement les réalités de la cybersécurité de la finance numérique.

L'étude dresse un tableau convaincant de la gestion des risques qui peine à suivre le rythme des complexités modernes. Au cœur de cette situation se trouve un décalage croissant entre les cadres traditionnels de gestion des risques et les menaces interconnectées d'aujourd'hui - un décalage brutalement mis en évidence par des catastrophes telles que Fukushima, où les défaillances en cascade ont défié l'analyse conventionnelle. Si les chercheurs proposent des outils plus dynamiques tels que les arbres d'attaque (Le Coze, et al., 2020) et les approches itératives du risque informatique (AFNOR, Gestion des risques projet IT, 2003), ces innovations restent confrontées aux cybermenaces alimentées par l'IA et à l'évolution fulgurante de secteurs tels que la banque en ligne. Les études révèlent deux points de consensus essentiels : premièrement, la numérisation et la mondialisation ont créé de nouvelles dimensions de risque nécessitant des solutions interdisciplinaires ; deuxièmement, les facteurs humains - des tâches aveugles cognitives à l'inertie institutionnelle - sapent constamment même les protocoles les plus sophistiqués.

Cette revue de littérature se positionne ainsi à l'intersection entre théorie établie et défis émergents, révélant un paradoxe central : la tension entre innovation technologique et contrôle des risques dans le secteur bancaire numérique. Elle adopte une perspective critique qui souligne les limites des modèles existants face aux évolutions rapides des technologies et des menaces, notamment en matière de cybersécurité.

## Section 2 : Cadre conceptuel de l'étude

### Partie 1 : Concepts fondamentaux du management de projet

#### 1. Définition et composantes du management de projet

##### a) Définition de projet et processus

Selon (institute, 2013) le projet est une entreprise temporaire pour créer un produit, un service ou un résultat unique. la nature temporaire des projets indique qu'un projet a un début et une fin définis. la fin es atteinte lorsque les objectifs du projet ont été atteinte ou lorsque le projet est terminé parce que ses objectifs seront ou ne peuvent pas être atteints, ou lorsque le besoin du projet n'existe plus.

Par contre un processus est un ensemble d'action et d'activités interdépendante réalisées pour créer un produit, un service ou un résultat prédéfini. Chaque processus est caractérisé par ces intrants, les outils et techniques applicables, et les extrants qui en résultent.

Le Management project est défini basé sur (PMI, A guide to the project management body of knowledge (PMBOK), 2004) "*A project in an organisation is a temporary endeavour undertaken to deliver a result.*"

Selon (Stanisław , 2016), les projets sont définis comme « *des activités mises en œuvre regroupées en processus à des intervalles prédéterminés, vérifiant l'état du projet et prenant des décisions critiques basées sur ces informations, en particulier en ce qui concerne leur initiation, et vérifiant la pertinence de continuer à mettre en œuvre le projet pendant sa mise en œuvre.* »

Une autre définition donnée par (Project Mnagement Institute (PMI), 2017). Un projet qui respecte les résultats déclarés tout en maintenant un budget, un calendrier et des contraintes de qualité peut ne pas être bon si les résultats souhaités ne sont pas atteints.

Le management de projet, comme défini dans la norme (AFNOR N. , X50-105 Août), comporte deux fonctions : la direction de projet et la gestion de projet. Il est indiqué dans cette norme que la direction de projet, pour prendre ses décisions de nature stratégique vis à vis du projet, a besoin des données recueillies et traitées par la gestion de projet.

Aussi la haute direction considère la gestion de projet comme « *une discipline axée sur l'exécution, complètement séparée des procédures de formulation et de mise en œuvre de la stratégie* » selon ( Musawir, Abd-Karim, & Mohd-Danuri).

**b) Le triangle des contraintes**

(AFNOR, 2010) À mesure que les projets avancent, les objectifs principaux de leur système deviennent essentiels pour orienter les efforts vers le succès :

1. Assurer la qualité des livrables du projet.
2. Gérer les coûts du projet pour rester dans un budget défini, afin d'atteindre les marges bénéficiaires souhaitées.
3. Respecter le calendrier du projet, avec l'objectif de le terminer à une date précise (D).
4. Maintenir des normes élevées dans les processus de gestion de projet.
5. Atteindre des résultats de performance supplémentaires, tels que des avantages sociétaux ou environnementaux.

Les trois premières valeurs proposées (GIARD, 1999) constituent ce que l'on appelle la triple contrainte ou le triangle de fer ( Atkinson, 1999). De plus, le système de projet se concentre sur plusieurs objectifs clés, collectivement appelés le pôle téléologique. Ces objectifs incluent la garantie de la qualité des livrables du projet, la gestion des coûts pour rester dans un budget spécifique et atteindre la rentabilité, ainsi que le respect d'un calendrier visant à terminer le projet à une date fixée (D).

Projet scope est défini comme le travail qui doit être effectué en suivant certaines spécifications et caractéristiques pour livrer un produit, un périmètre bien défini est crucial pour le succès du projet (Project Management Institute, 2000; Roger , Crawford, & Ward, 2006).

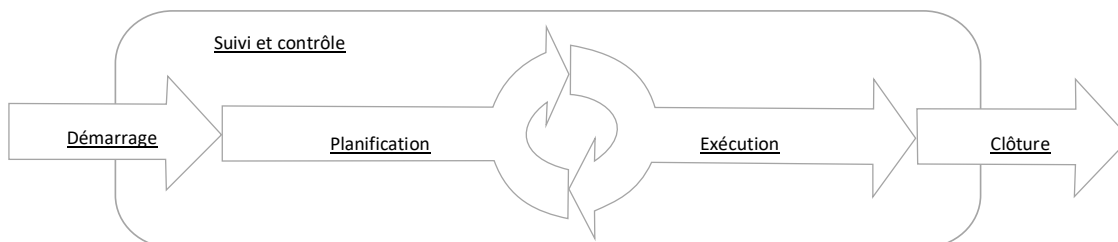
**c) Parties prenantes et leurs rôles dans la gouvernance du projet**

Selon (Institute, 2017) « processus requis pour identifier les personnes, les groupes ou les organisations susceptibles d'affecter ou d'être affectés par le projet, pour analyser les attentes des parties prenantes et leur impact sur le projet, mais aussi pour développer des stratégies de gestion appropriées afin de mobiliser efficacement les parties prenantes en les impliquant dans les décisions du projet et son exécution. Ces processus permettent à l'équipe projet d'analyser les attentes des parties prenantes, d'évaluer dans quelle mesure elles affectent ou sont affectées par le projet et d'élaborer des stratégies afin de les faire participer de manière efficace dans la prise de décision du projet mais aussi la planification et l'exécution du travail du projet. »

## 2. Cycle de vie d'un projet

Le MP comprend cinq étapes (Démarrage, Planification, Exécution, Suivi et Contrôle, Clôture) avec des interfaces et des flux d'information clairement définis :

**Figure 1:** Processus général de management de projets



**Source :** Groupe de processus du management de projets (PMI, Project Management Institute, 5 édition., 2014)

Ces processus visent à simplifier l'application des connaissances, des outils et des techniques, tout en assurant et en soutenant l'avancement harmonieux et efficace du projet à chaque étape de son cycle de vie.

Donc, la gestion d'un projet se réalise par l'incorporation de ces cinq processus complémentaires.

Le processus de Management des risques présenté sur la Figure (1) ci-après est composé des actions suivantes :

Ces processus visent à simplifier l'application des connaissances, des outils et des techniques, tout en assurant et en soutenant l'avancement harmonieux et efficace du projet à chaque étape de son cycle de vie.

Donc, la gestion d'un projet se réalise par l'incorporation de ces cinq processus complémentaires.

**Démarrage :** Ce processus vise à définir un nouveau projet, ou une phase émergente d'un projet existant et de présenter l'ensemble des informations nécessaires pour obtenir l'autorisation de démarrage du projet. Dans ce processus, il faut spécifier clairement la justification et l'origine du projet, les ressources à prévoir, ainsi que l'identification du chef de projet. Cette affectation de responsabilité fait l'objet d'une charte projet regroupant toutes les informations et qui doit être signée par le sponsor du projet.

Planification : ce processus vise à définir l'ensemble des phases, activités et jalons nécessaires pour transformer les attentes des clients à l'origine du projet, en leur satisfaction. Le processus consiste à établir une décomposition successive des livrables à fournir en éléments plus simples à appréhender selon le principe de Descartes, puis à identifier les actions à mener et leurs dépendances pour être en mesure d'élaborer chacun des livrables. L'ensemble des actions à mener sont, par la suite, ordonnancées en intégrant les ressources et les budgets nécessaires. Le résultat est le plan du projet qui constitue la feuille de route à suivre.

Exécution : ce processus rassemble l'ensemble des tâches à mener pour accomplir le travail ayant été défini lors du plan de projet, tout en respectant les spécifications et les exigences du projet. Dans ces processus vont être exécutées :

- Les actions qui ont été planifiées au préalable dans le plan de projet,
- Les actions correctives ayant été prévues ou pas dans le plan de projet, en tenant compte des dérives des objectifs et du plan de projet.

Suivi et contrôle : ce processus vise à suivre, à revoir et à réguler l'avancement et les performances du projet. Il vise aussi à identifier les « emplacements » dans le plan de projet initial où des modifications sont obligatoires, et de faire les ajustements nécessaires. Le processus consiste à mesurer de façon régulière l'avancement du projet en termes de coût, de délai, de ressources et de livrables, et à définir les corrections nécessaires pour revenir à une situation acceptable. De plus, lors des processus de suivi, la direction doit constituer un système de contrôle axé sur la bonne exécution du projet, à travers l'emploi d'outils spécifiques de maîtrise de risques et de gestion des conflits et des problèmes, pour atteindre les objectifs attendus du projet. Il est à noter que ce processus de Suivi et Contrôle du projet sera une cible privilégiée dans la suite de nos travaux.

Clôture : ce processus vise, dans tous les groupes de processus, à clore officiellement toutes activités du projet ou d'une phase du processus. Le processus consiste à vérifier l'acceptation formelle des différents livrables et l'exhaustivité des documents relatifs à la clôture des tâches et phases.

Cette modélisation du management de projet, basée sur cinq processus interactifs, peut être appliquée intégralement à divers types de projets. Elle peut également s'adapter à certaines phases, sous des conditions spécifiques, telles que la gestion par une équipe distincte, la

clôture dépendant d'un jalon décisionnel, ou encore une planification partielle lorsque le projet ne permet pas une planification complète dès le départ jusqu'à son achèvement (PMI, Project Management Institute, 5 édition., 2014).

### **3. L'importance de la gestion des risques dans un projet**

selon ( Gourc & Bougaret, LE MANAGEMENT DES RISQUES APPLIQUE AU MANAGEMENT DES PROJETS ET DE PORTEFEUILLE DE PROJETS EN RECHERCHE ET DEVELOPPEMENT, 1999)

- fournir une meilleure connaissance de la situation du projet et de son niveau d'exposition au risque par la mise à disposition d'indicateurs complémentaires pertinents,
- améliorer l'anticipation et la réactivité des équipes projet à la survenue des événements redoutés,
- participer à une meilleure définition de la cible du projet à son lancement, mais également tout au long du projet par une réactualisation périodique en fonction du degré de connaissance croissant du projet.

### **4. Les approches de gestion de projet**

#### **a) Approche prédictive (traditionnelle/en cascade)**

La méthode en cascade, également connue sous le nom de Waterfall, a été introduite par Herbert D. Benington en 1956 lors d'un symposium sur les méthodes de programmation avancées. Elle repose sur une approche séquentielle rigoureuse qui divise le projet en phases distinctes et interdépendantes, chacune devant être achevée avant de passer à la suivante.

L'une des caractéristiques fondamentales de cette méthode est son irréversibilité : une fois qu'une phase est validée, il n'est pas possible de revenir en arrière. Ainsi, en cas de problème, l'unique recours consiste à reprendre le processus depuis le début, ce qui exige une planification minutieuse dès les premières étapes.

Pour garantir l'efficacité de cette approche, il est essentiel de définir clairement les exigences du projet dès l'amont, en tenant compte des objectifs et des contraintes. Une implication active des acteurs est également requise, chaque membre devant comprendre son rôle et contribuer pleinement à la réussite du projet. Enfin, une documentation exhaustive joue un

rôle clé dans la coordination des équipes, permettant de maintenir une cohérence opérationnelle tout au long du cycle de développement. (projet, 2024).

### **b) Approche agile**

« Nous découvrons comment mieux développer des logiciels par la pratique et en aidant les autres à le faire. » *Extrait du Manifeste Agile.*

Appliquée au monde des logiciels (Khalil, 2011), la notion d'agilité renvoie à la capacité d'adaptation des sociétés informatiques aux demandes évolutives des clients, arrivant le plus souvent en cours de projet et à une meilleure maîtrise du triptyque « coût/qualité/périmètre fonctionnel ». Ces méthodes constituent une nouvelle logique de développement de projets informatiques, décrites comme étant itératives, incrémentales, encourageant l'auto organisation et l'adaptation au changement.

#### **• Principes et valeurs (Manifeste Agile)**

Selon. (El Allame, Blog gestion de projet, s.d.), L'Agilité repose sur quatre principes essentiels qui redéfinissent la gestion de projet. Les individus et leurs interactions sont au cœur du succès d'une organisation, bien plus que les processus et les outils. Une équipe motivée et impliquée est le véritable moteur de la performance, tandis que les méthodes de travail doivent rester simples et adaptées aux besoins réels.

L'efficacité opérationnelle prime sur une documentation exhaustive. L'Agilité privilégie des documents concis et structurés, intégrant les informations essentielles sans alourdir les processus. La documentation est divisée en deux catégories : celle qui concerne les exigences du produit et celle qui détaille les aspects techniques, garantissant ainsi une approche pragmatique et fluide.

La collaboration avec les clients est un autre pilier fondamental. Plutôt que de s'enfermer dans des négociations contractuelles rigides, la méthode Agile valorise une interaction continue avec les utilisateurs. Chaque retour est une opportunité d'optimisation, permettant d'ajuster le produit en fonction des besoins évolutifs. Cette démarche flexible assure un alignement constant entre la conception et les attentes du marché.

Enfin, l'adaptation au changement est privilégiée par rapport à un suivi strict d'un plan prédéfini. La capacité d'ajustement et d'anticipation est essentielle pour garantir la stabilité du projet face aux imprévus. Grâce à une approche proactive, les équipes peuvent réagir rapidement aux nouvelles exigences, sans compromettre la cohérence du développement.

- **La méthode « scrum »**

Cette méthode est largement adoptée dans les milieux académiques et professionnels, offrant une approche spécifique et complémentaire pour la gestion agile des projets informatiques. Son application permet d'adapter efficacement le développement aux exigences évolutives tout en optimisant les processus de collaboration et de livraison.

Les auteurs se réfèrent au concept « scrum » pour souligner une approche de développement permettant d'améliorer la cohésion de l'équipe et la rapidité du processus de développement (Takeushi & Nonaka, 1986).

Scrum est une méthode agile qui optimise la collaboration et la gestion des projets grâce à des principes clés comme la transparence, l'inspection et l'adaptation. Elle repose sur des sprints, des cycles de travail courts, et des réunions quotidiennes pour assurer une communication efficace. Trois rôles majeurs structurent Scrum : le Scrum Master, qui facilite le processus, le Product Owner, qui définit et priorise le backlog pour maximiser la valeur du produit, et l'équipe de développement, chargée de livrer des incréments de produit à chaque sprint. Cette approche flexible permet d'adapter les projets aux évolutions et aux contraintes tout en garantissant leur bon déroulement.

- c) **Approche hybride**

(Tanzeem, Ravi, Subrahmanyasarma, Yellepeddi, & Pamidi Venkata, 2018) La gestion de projet hybride représente une approche méthodologique qui intègre éléments à la fois traditionnels et agiles cadres de gestion de projet pour optimiser la livraison des projets et l'adaptabilité.

Ce concept émerge de la reconnaissance qu'aucune méthodologie unique ne suffit à aborder toutes les complexités et exigences dynamiques des projets contemporains. En combinant la nature structurée, nature séquentielle des méthodes traditionnelles avec les attributs itératifs et flexibles de pratiques agiles, la gestion de projet hybride vise à offrir une approche plus polyvalente et efficace pour gérer des projets diversifiés.

La gestion de projet hybride constitue une approche combinant les méthodologies traditionnelles et agiles afin de pallier leurs limites lorsqu'elles sont utilisées isolément. Cette approche repose sur la reconnaissance de la complexité croissante des projets modernes, nécessitant une structuration rigoureuse pour garantir la stabilité, tout en intégrant une flexibilité adaptative afin de répondre aux évolutions du marché et aux nouvelles exigences.

## **5. Importance de la gestion des risques dans un projet**

L'adoption d'une démarche structurée de management des risques revêt une importance, Dans ce contexte, une approche proactive des risques permet notamment de : ( Gourc & Bougaret, LE MANAGEMENT DES RISQUES APPLIQUE AU MANAGEMENT DES PROJETS ET DE PORTEFEUILLE DE PROJETS EN RECHERCHE ET DEVELOPPEMENT, 1999):

- Elle permet tout d'abord d'offrir une vision plus précise de la situation du projet et de son niveau d'exposition aux risques, en mettant à disposition des indicateurs complémentaires pertinents.
- Elle contribue également à renforcer l'anticipation et la réactivité des équipes face aux événements critiques, facilitant ainsi une meilleure gestion des imprévus et une réduction des impacts négatifs.
- Par ailleurs, la gestion des risques soutient une définition plus précise des objectifs du projet, dès son lancement mais aussi tout au long de son cycle de vie, grâce à une mise à jour régulière des informations en fonction de l'évolution du projet et de la compréhension accrue des enjeux.
- En définitive, cette approche permet d'affiner la prise de décision en réduisant les risques d'erreur, tels qu'une surestimation des coûts ou des délais, ou une évaluation erronée de la faisabilité du projet. Elle garantit ainsi une allocation optimale des ressources et une meilleure maîtrise des incertitudes.

## **Partie 2 : Gestion des risques en management de projet**

### **5. Définition et concepts clés**

#### **a) Notion de risque, menace et opportunité**

Selon (AFNOR, 2010) un risque est « l'effet de l'incertitude sur l'atteinte des objectifs ».

Le Management des Risques est avant tout un processus spécifique déployé pour faire face aux nombreuses incertitudes d'un projet. Ce processus préventif vise à ( Larson & Gray, 2013) :

- Éliminer les menaces (événements indésirables) ou minimiser leurs conséquences négatives sur la capacité du projet à atteindre les objectifs et à respecter les obligations.

- Promouvoir les opportunités (événements désirables) ou maximiser leurs conséquences positives.

Pour ( Manotas Niño, 2017) le risque se définit comme un événement dont la survenue est probable et susceptible d'avoir un impact sur la capacité d'un système ou d'une organisation à atteindre ses objectifs ou à remplir ses obligations. Cet impact peut être positif, lorsqu'il crée de nouvelles opportunités et favorise l'innovation, ou négatif, lorsqu'il engendre des menaces susceptibles de perturber le fonctionnement prévu. Ainsi, la gestion du risque consiste à anticiper ces événements, à en évaluer les effets potentiels et à mettre en place des stratégies adaptées pour minimiser les impacts négatifs tout en capitalisant sur les opportunités.

Souvent, là où se trouve un risque, il y a également une opportunité. Toute opportunité devrait être soumise à une évaluation des risques associés pour déterminer si elle est véritablement avantageuse. On peut observer plusieurs liens entre les dangers relevés au sein d'une société et les opportunités qu'ils suscitent. ( Ivascu & Cioca, 2014)

La notion de risque positif et d'opportunité en gestion de projet repose sur l'idée que certains risques, bien que présentant une incertitude, peuvent générer des avantages stratégiques et des opportunités de croissance. Contrairement aux risques purement négatifs, les risques positifs sont des événements incertains qui, s'ils se réalisent, peuvent améliorer la performance du projet ou offrir un avantage compétitif.

## **6. Objectifs et principes du management des risques**

La norme (31000, 2018 ) ISO 31000 versions 2018 fournit un cadre de management des risques qui peut être appliqué à toute organisation, secteur ou contexte. Selon cette norme, les objectifs de management des risques sont les suivants :

a) Protéger la valeur et l'image de l'organisation : le management des risques permet d'identifier et de prévenir les événements qui pourraient nuire à la réputation de l'organisation, à son image de marque, à sa crédibilité, à sa capacité à maintenir la confiance de ses parties prenantes et à sa capacité à réaliser ses objectifs.

b) Améliorer la prise de décision : le management des risques permet de fournir des informations pertinentes et fiables sur les risques encourus par l'organisation, ce qui permet de prendre des décisions éclairées et de hiérarchiser les actions à entreprendre.

c) Améliorer la résilience de l'organisation : le management des risques permet de prévenir les perturbations et de réduire l'impact des événements indésirables sur l'organisation, ce qui renforce sa capacité à faire face aux situations difficiles et à s'adapter aux changements.

d) Optimiser les opportunités : le management des risques permet de repérer les opportunités qui se présentent à l'organisation et de les exploiter de manière efficace, ce qui permet de tirer parti des avantages concurrentiels et de renforcer la position de l'organisation sur le marché.

e) Améliorer la confiance des parties prenantes : le management des risques permet de démontrer la capacité de l'organisation à anticiper et à manager les risques, ce qui renforce la confiance des parties prenantes (clients, employés, actionnaires, régulateurs, etc.) dans l'organisation.

## 7. Typologie des risques dans la gestion de projet

Tout projet de réalisation d'un système est soumis à des aléas susceptibles ayant un impact négatif sur le succès global du projet, des résultats spécifiques, ou des événements pouvant créer des dommages imprévisibles. Ce sont les « risques projet » qui sont d'après plusieurs auteurs comme suit (Dr. Menaouer):

- **Risques techniques** : L'utilisation d'un nouveau langage informatique ou d'une technologie émergente peut poser des défis majeurs, notamment lorsque les équipes ne maîtrisent pas encore ces outils. De plus, l'absence de références normatives et standards clairement définis peut compliquer l'intégration et la compatibilité des solutions développées.
- **Risques humains** : L'absence imprévue d'un membre clé du projet, qu'elle soit due à une maladie, un départ volontaire ou une réaffectation à d'autres priorités organisationnelles, peut affecter la dynamique de travail. Par ailleurs, un manque de compétences par rapport aux exigences du projet ou la survenue de conflits internes peuvent nuire à la progression des travaux.
- **Risques juridiques** : Un partenaire contractuel (fournisseur, prestataire) peut être confronté à des difficultés telles qu'une faillite, entraînant un impact direct sur les engagements du projet. Les contraintes liées aux lois et réglementations en vigueur, notamment en matière de langue et de cadre juridique applicable, doivent être soigneusement prises en compte.

- **Risques liés aux délais** : Une sous-estimation initiale du temps nécessaire à l'exécution des tâches peut générer des retards et compromettre le respect du planning établi.
- **Risques intrinsèques à la gestion de projet** : Une répartition inadéquate des responsabilités ou une organisation floue des rôles peuvent engendrer des inefficacités. De même, une implication insuffisante des parties prenantes, notamment des commanditaires, peut limiter la prise en compte des attentes et des objectifs stratégiques.
- **Risques liés au management** : Un suivi insuffisant du projet peut empêcher la détection précoce des dérives et limiter la réactivité face aux aléas. L'absence d'un mécanisme efficace de contrôle et d'ajustement peut compromettre la bonne exécution du projet.

Ces risques peuvent être regroupés en deux grandes familles : les risques externes (exogènes) et les risques internes (endogènes). Les risques projet sont recensés par le chef de projet dans le registre des risques, puis sont suivis au quotidien. Une réponse spécifique est apportée à chaque risque, afin d'éviter qu'il apparaisse. Ces réponses sont inscrites dans le plan de prévention des risques.

Il existe deux grandes familles de risques :

- Les risques exogènes :

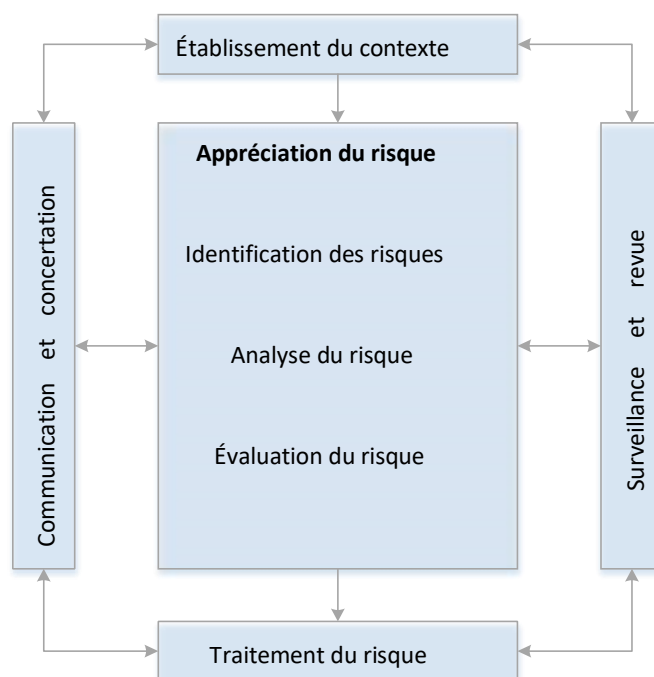
Il s'agit des risques extérieurs à l'entreprise. Par exemple : évolution de la réglementation, délais supplémentaires de livraison côté fournisseur, pandémie mondiale, risques politiques et sociaux, météo.

- Les risques endogènes :

Il s'agit des risques internes à l'entreprise. Par exemple : organisation du projet, indisponibilités des experts, mauvaises estimations, choix des prestataires.

## **8. Processus de gestion des risques**

L'objectif principal de l'évaluation des risques au sein des entreprises consiste à identifier les facteurs de risque liés au marché, à analyser leur impact sur la pérennité des bénéficiaires, et à mesurer les conséquences de ces risques. Il est impératif pour les entreprises de maintenir une vigilance constante face aux risques et de développer des stratégies efficaces pour atténuer leur influence sur les activités commerciales. Cependant, cette démarche exige une approche systématique et adaptée aux spécificités de chaque organisation. Selon la Norme ISO 31000, le processus de Management des risques présenté sur la Figure ci-après est composé des actions suivantes :

**Figure 2:** Processus général de management des risques

Source : ( AFNOR, 2010))

Établissement du contexte : cette activité vise à définir les éléments à prendre en compte dans l'étude, à savoir les objectifs du Management des risques, les cibles et le contexte de l'analyse des risques à mener. Elle permet aussi de préciser la méthode de cotation (critères permettant de définir l'importance du risque). De cette action, il est découlé une note de cadrage permettant de statuer sur le contexte de l'étude.

- Appréciation des risques : cette partie de la démarche comporte la recherche, la reconnaissance et l'enregistrement des risques pouvant affecter le contexte d'étude considéré. Le but est d'identifier les raisons pour lesquelles les objectifs de la cible considérée pourraient ne pas être atteints ou pourraient être plus facilement atteints. Elle est composée des activités suivantes :
- Identification des risques : cette activité consiste à faire un inventaire de tous les risques susceptibles d'affecter le bon déroulement de l'organisation considérée et de documenter leurs caractéristiques. Il existe plusieurs outils pour structurer et formaliser l'identification des risques, comme par exemple : l'analyse documentaire systématique, la technique Delphi, les interviews, les analyses Strengths (forces), Weaknesses (faiblesses), Opportunities (opportunités), Threats (menaces) (SWOT), le diagramme d'Ishikawa ou les diagrammes d'influence. L'identification des risques est un travail

complexe car il existe une grande variété d'événements potentiels pouvant avoir un impact positif ou négatif sur le respect des objectifs. Cette identification est donc un travail d'équipe qui nécessite l'engagement de plusieurs experts métier ayant déjà œuvré dans des contextes d'étude similaires au contexte courant.

- Analyse des risques : cette activité consiste à comprendre le risque, c'est-à-dire à préciser l'événement redouté, les causes d'apparition, les conséquences à la suite de son apparition et la capacité du système ou de l'organisme étudié à détecter le risque avant ou après son apparition. L'objectif est d'attribuer, à chaque risque identifié, un niveau de risque afin de les hiérarchiser. Face à la grande diversité de risques, il est nécessaire de mettre en place un référentiel d'évaluation fiable, capable de classer quantitativement ou qualitativement les risques par ordre d'importance. Il est à noter que le niveau de risque dépend du contexte et des cibles étudiées.
- Évaluation des risques : l'objectif est, à partir de la classification des risques selon leur niveau de criticité, de permettre aux experts de déterminer les risques qui nécessitent un traitement prioritaire dans la mise en œuvre des actions de contrôle. L'objectif est de comparer les résultats de l'analyse du risque avec les critères de risque et de déterminer quel risque n'est pas acceptable. Il permet de déterminer un « seuil de tolérance ou significativité » au-dessus duquel le traitement est obligatoire.
- Traitement des risques : cette activité vise à définir et à détailler les actions de maîtrise ou de mitigation à entreprendre avec la définition des pilotes (personnes responsables de l'implémentation), du coût et délai de réalisation, des moyens nécessaires et des éléments déclencheurs. Il est à noter que certaines actions sont curatives, c'est-à-dire qu'elles ne sont mises en œuvre qu'après détection du problème, problème correspondant à la concrétisation d'un risque. Pour cela, il est possible d'adopter une stratégie appropriée parmi les six types de stratégie de gestion du risque :
  - l'acceptation du risque : cette attitude consiste à délibérément n'engager aucune action spécifique pour se protéger contre un risque donné,
  - l'annulation du risque : cette stratégie consiste à revoir la cible en termes d'objectifs à atteindre, de solutions techniques déployées, d'organisation des tâches ou d'affectation des ressources de sorte, soit à faire disparaître le risque, soit à protéger les objectifs ou les rendre insensibles à l'occurrence du risque,

- la prévention du risque : cette stratégie consiste à trouver des solutions ou des moyens pour amener la probabilité d'occurrence du risque en dessous d'un seuil acceptable,
  - la protection du risque : cette stratégie consiste à trouver des solutions ou des moyens pour réduire la gravité, c'est-à-dire les conséquences sur les objectifs et/ou obligations,
  - la surveillance du risque : cette stratégie vise à identifier les symptômes précurseurs permettant de prédire l'apparition d'événements déclencheurs et de les surveiller,
  - le transfert du risque : cette dernière stratégie consiste à trouver une tierce partie qui accepte de prendre à son compte les conséquences de l'occurrence du risque. Cette tierce partie devient alors propriétaire des plans de réponse du risque en question. Par ce biais, le risque n'est pas éliminé mais les conséquences sont gérées par un tiers, moyennant une contrepartie financière.
- Surveillance et revue : cette activité consiste d'une part, à vérifier que le déploiement des actions de maîtrise est conforme aux décisions prises et, d'autre part, à rendre compte à la direction des progrès et avancées suite au déploiement des actions de maîtrise et à évaluer la performance, la cohérence et les écarts par rapport à l'efficacité du changement. Par ailleurs, la norme établit que cette activité doit être un processus de contrôle en continu accompli pendant tous les processus de Management des risques afin d'identifier des opportunités d'amélioration et d'apprentissage de nouvelles connaissances.
  - Communication et concertation : cette activité transversale a pour finalité d'élaborer des plans de « communication et de concertation » avec les parties prenantes. En effet, il est important de mettre en place un système d'échange d'informations avec des protocoles suffisants pour que les acteurs impliqués dans le processus de Management des risques puissent confronter et connaître l'ensemble des points de vue et des actions ou décisions en cours (AFNOR, 2010).

## **9. Particularités de la gestion des risques selon l'approche de projet**

### **a) Gestion des risques dans l'approche prédictive**

Divers modèles théoriques ont longtemps guidé la gestion des risques, chacun proposant une approche distincte pour détecter, apprécier et gérer les risques éventuels. Dans ce domaine, une des méthodes essentielles est le système d'Évaluation et de Gestion des Risques (RAM),

qui met l'accent sur l'identification, l'évaluation et la hiérarchisation des risques avant de répartir judicieusement les ressources pour réduire, surveiller et maîtriser leur probabilité ou leur incidence.

Dans ce processus, l'analyse prédictive tient une place primordiale en s'appuyant sur des données historiques et actuelles pour perfectionner les estimations de risques. En perfectionnant la précision dans la hiérarchisation des risques, cela renforce les stratégies de réduction, augmentant leur efficacité et leur fondement sur des données concrètes. (Familoni & Shoetan, 2024).

#### **b) Gestion des risques dans l'approche agile**

Le succès d'un projet agile repose sur une gestion efficace des risques. Étant donné que la gestion des risques est un facteur crucial pour assurer la mise en œuvre fluide des projets, les méthodologies agiles l'adoptent comme un principe fondamental. Les stratégies et méthodes décrites dans cet article ( Suvvari, 2020) aident les équipes à identifier, évaluer et traiter proactivement les risques tout au long du cycle de vie du projet. En intégrant la gestion des risques dès le début, les équipes peuvent s'adapter rapidement aux changements, atténuer les pièges potentiels et protéger à la fois leur flux de travail et le succès du projet. Cette approche tournée vers l'avenir rend la gestion des risques en agile non seulement bénéfique mais essentielle.

#### **c) Gestion des risques dans l'approche hybride**

Certains aspects d'un projet nécessitent une structure rigide et bien définie, comme la documentation ou les exigences légales, tandis que d'autres, comme le développement de nouvelles fonctionnalités, exigent plus de souplesse.

Pour réduire les risques, une approche hybride permet de démarrer avec le modèle Waterfall afin de clarifier les attentes et anticiper les obstacles, puis de passer à l'Agile pour adapter le développement en fonction des retours et des évolutions. Ce processus aide l'équipe à éviter les erreurs et à garantir la conformité tout en restant réactive aux changements. (Germain, 2025).

### **Partie 3 : Outils et approches clés pour la gestion des risques**

#### **1. Méthodes et outils traditionnelles de gestion des risques**

##### **a) L'approche fonctionnelle**

L'approche fonctionnelle repose sur le principe de séparabilité des fonctions, une notion qui s'appuie sur les fondements du raisonnement cartésien. Selon cette perspective, l'analyse d'un phénomène ou la résolution d'un problème passe par sa décomposition en éléments plus simples, permettant une étude plus approfondie et structurée.

Dans le cadre de ses travaux sur l'élaboration d'une théorie générale du risque, ( Bouyssou, 1997) adopte une approche fortement inspirée du Discours de la Méthode de Descartes, mettant en avant quatre préceptes fondamentaux pour guider la réflexion :

1. Structurer sa pensée de manière ordonnée, afin de garantir une progression cohérente dans l'analyse.
2. Décomposer les difficultés en sous-problèmes distincts pour mieux en appréhender les enjeux.
3. S'assurer de la clarté et de la validité des affirmations, évitant ainsi toute conclusion fondée sur des éléments incertains.
4. Procéder régulièrement à une évaluation critique des réflexions menées, afin de garantir un raisonnement ajusté et pertinent.

##### **b) L'approche stratégique**

La gestion des risques stratégiques vise à identifier, évaluer et atténuer les risques liés aux décisions stratégiques d'une entreprise, afin de garantir son adaptabilité à un environnement concurrentiel en constante évolution ( Pierandrei, 2019).

Les premiers travaux dans ce domaine remontent au XXe siècle, initiés par des dirigeants d'entreprise soucieux de protéger leurs organisations des conséquences potentielles des fluctuations économiques, politiques et sociales. Ces recherches ont conduit au développement de plusieurs méthodes et outils fondamentaux, grâce aux contributions de chercheurs tels qu'Igor Ansoff, Henry Mintzberg et Peter Drucker. Parmi les approches les plus reconnues, on retrouve (FATOUH, 2023):

- L'analyse SWOT, qui permet d'évaluer les forces, faiblesses, opportunités et menaces susceptibles d'influencer la performance d'une entreprise.

- Le modèle des cinq forces de Porter, utilisé pour examiner l'intensité concurrentielle au sein d'un secteur et identifier les facteurs influençant la rentabilité.
- L'analyse PESTEL, qui aide à comprendre l'impact des facteurs macro-environnementaux (politiques, économiques, socioculturels, technologiques, écologiques et légaux) sur la stratégie d'une organisation.

### c) L'approche analogique

Dans (Gidel & Zonghero, 2006) les auteurs proposent une typologie des méthodes d'identification des risques :

L'approche analogique basée sur l'étude des expériences des projets passés. L'inconvénient est qu'elle ne prend en considération que les risques déjà identifiés et enregistrés dans des projets similaires.

### d) L'approche analytique

L'approche analytique basée sur une analyse détaillée et systématique des risques des composants basiques du projet (tâches, livrables, ressources...). Les méthodologies idoines sont l'AMDEC et l'arbre de défaillance. Ce cadre fournit une variété de modèles et d'outils pour soutenir la gestion des risques, Cela inclut :

**Un registre des risques** : Dans le PMBoK, le registre des risques est défini comme un document dans lequel les résultats de l'analyse des risques et de la planification des réponses aux risques sont consignés (A Guide to the Project Management Body of Knowledge, 2013).

**Une liste de contrôle des risques** : L'outil d'évaluation des risques du laboratoire de Stanford fournit un cadre pour l'évaluation des risques qui s'aligne sur la méthode scientifique, s'intégrant au processus que les chercheurs utilisent déjà pour répondre aux questions scientifiques. Cet outil permet aux chercheurs d'identifier et de contrôler systématiquement les dangers afin de réduire le risque de blessures et d'incidents. Réalisez une évaluation des risques avant de mener une expérience pour la première fois. (Laboratory Risk Assessment Tool, 2021)

### e) La méthode de cotation des risques

La cotation d'un risque se définit comme un processus d'évaluation quantitative des impacts possibles liés à l'apparition d'un risque, en tenant compte de son influence sur l'atteinte des objectifs et le respect des obligations. Cette cotation repose traditionnellement sur trois critères principaux (Patricia & Niño, 2017):

- La gravité (G) ou l'impact, qui représente les pertes ou les gains potentiels relatifs à la réalisation des objectifs (tels que financiers, image de marque, livrables, délais) ainsi qu'à la satisfaction des obligations (contenu, coût, délai).
- La probabilité d'occurrence (O), qui évalue la probabilité que l'événement, qu'il soit redouté ou recherché, se produise.
- La détectabilité (D) ou contrôlabilité, qui mesure la probabilité de détecter le risque avant son apparition (symptômes précurseurs), pendant (manifestation en cours) ou après (effets constatés).

#### **f) Matrices d'évaluation des risques**

Selon (El Allame, s.d.) La matrice de criticité est un outil essentiel en gestion de projet permettant d'évaluer et de classer les risques susceptibles d'affecter un projet ou une organisation. Utilisée à différentes étapes du processus décisionnel, elle se présente sous forme d'une grille où la probabilité d'occurrence d'un risque est représentée sur un axe, tandis que son impact potentiel figure sur l'autre. Les niveaux de probabilité, généralement définis de faible à élevé, sont mis en relation avec les degrés de gravité des conséquences, allant de mineures à critiques, voire catastrophiques. Chaque cellule de la matrice indique ainsi le niveau de risque correspondant à une combinaison donnée de probabilité et d'impact, facilitant l'identification des priorités et l'élaboration de stratégies de gestion des risques adaptées.

#### **g) Le diagramme de Pareto**

Le diagramme de Pareto (Pommeret, 2017) est un outil qui nous aide via la méthode ABC à hiérarchiser des éléments sur des bases chiffrées sur des critères importants pour faire des choix. Par exemple, quand on mène une résolution de problème en groupe de travail, il arrive un moment où on peut avoir listé beaucoup de causes à ce problème. Si on cherche à toutes les éliminer, on va dépenser de l'énergie, parfois pour des causes très rares. Avec le diagramme de Pareto, on identifiera les principales sur lesquelles agir. Cet outil vise à fournir

une représentation visuelle d'un classement décroissant en fonction de l'importance relative des défauts, des causes ou des dysfonctionnements. Ce classement repose sur des critères quantitatifs, tels que la fréquence d'apparition, le coût, le nombre d'occurrences, ou encore les résultats d'un vote.

#### **h) Les méthodes de cartographie des risques**

Les méthodes de cartographie des risques varient en matière d'objectifs organisationnels et de caractéristiques de performance (Guide IENA, 2017; De Santis, 2020) . Contrairement aux autres risques, le risque opérationnel n'est pas spécifique à un produit. Ainsi son analyse nécessite une compréhension de l'ensemble de l'activité de l'organisation (Scandizzo, 2005). Deux approches principales sont employées pour cette analyse : Top-down et Bottom-up.

- **L'approche Top-down** : Initiée par la direction générale, cette approche consiste à orienter et décliner les décisions stratégiques vers les différentes entités et services de l'organisation. Elle suit les étapes suivantes (IFACI, 2013):
- Présentation des risques et leur évaluation ;
- La comparaison de ces risques détectés avec la nomenclature des risques de l'entreprise ;
- Le rapprochement de ces risques avec les processus de l'entreprise ;

Cette méthode contribue à sensibiliser les parties prenantes aux risques opérationnels et constitue un outil d'information essentiel.

- **L'approche Bottom-up** : Axée sur une collecte d'informations remontant des différents départements à la direction générale, cette approche repose sur une analyse systématique des risques opérationnels et des contrôles associés à chaque processus identifié. Ses étapes incluent (IFACI, 2013) :
- Identification des processus.
- Identification et évaluation des risques à chaque niveau de processus.
- Analyse et évaluation des contrôles existants.
- Chiffrage du risque résiduel.

Ces deux approches permettent d'aborder les risques opérationnels selon des perspectives complémentaires, favorisant une compréhension approfondie et une meilleure gestion des incertitudes.

**i) La méthode Risk Breakdown Structure (RBS)**

Les risques peuvent être analysés à travers une représentation hiérarchique, permettant leur classification en grandes catégories, elles-mêmes subdivisées en sous-catégories pour identifier les domaines et les causes potentielles des risques. Cette méthode, appelée Risk Breakdown Structure (RBS) dans le monde anglo-saxon, consiste à hiérarchiser l'ensemble des risques par des catégories afin de pouvoir les présenter sous forme d'arbre. (Claire Choisy, 2020).

**j) La technique Simulation de Monte Carlo (MCS)**

Selon (S. Alessandria, 2018) La méthode proposée d'Évaluation Quantitative du Risque Sismique (QsRA) a été mise en œuvre numériquement par la technique de Simulation de Monte Carlo (MCS). La technique MCS génère des échantillons des variables aléatoires régissant les scénarios de dommages et l'analyse des conséquences. Chaque échantillon est basé sur des fonctions de distribution de probabilité prédéfinies, et des groupes de ces variables d'échantillon simulent des événements. En répétant les simulations MCS, une distribution de fréquence des résultats possibles est produite.

Le processus de simulation complet permet le calcul de plusieurs probabilités :

Probabilités d'occurrence de chaque événement initial et chaîne accidentelle.

Probabilités de dommages pour chaque unité ou composant.

Risques sociétaux tels que les probabilités de mortalité dans des zones spécifiques.

Impacts économiques, y compris les volumes de diffusion de contenu, les coûts de reconstruction et les interruptions d'activité.

**k) Le diagramme d'Ishikawa**

Selon (El Allame, Blog Gestion de Projet) Le diagramme d'Ishikawa, également appelé diagramme de causes à effets ou arbre Ishikawa, est un outil graphique permettant d'identifier et de visualiser les différentes causes potentielles d'un problème ou d'un effet indésirable. Son objectif principal est d'aider à détecter les causes profondes à l'origine d'une difficulté afin de faciliter la mise en place de solutions adaptées. Cette approche repose

sur une hiérarchisation des causes : les causes primaires, qui sont les premières sources du problème, engendrent des causes secondaires, souvent considérées comme les causes racines. Grâce à cette structuration, le diagramme d'Ishikawa offre une vision claire et méthodique des facteurs influençant un problème, facilitant ainsi son analyse et sa résolution.

Ci-après les 5 étapes pour présenter le schéma d'Ishikawa :

1. **À droite de la tête du poisson** : on marque l'effet observé, le problème à résoudre ou la situation à changer
2. **Sur les arêtes ou branches du poisson** : on indique les 5 grandes catégories de causes majeures à l'origine de l'effet, problème ou situation
3. **Sur chacune des branches du poisson** : on exprime les causes primordiales de l'effet, problème ou situation
4. **Par rapport à chaque cause primordiale** : on révèle les causes secondaires qui en sont responsables

Dans le cadre du management des risques, cet outil revêt une importance particulière puisqu'il sera appliqué concrètement à notre travail.

L'analyse des cinq M dans le cadre du diagramme d'Ishikawa permet d'identifier les facteurs clés influençant la réussite d'un projet, d'une mission ou d'un événement. Le premier élément, la main-d'œuvre, englobe toutes les personnes impliquées dans le processus. Il s'agit non seulement des compétences techniques et du niveau de connaissances des acteurs, mais aussi de leur motivation, leur influence, leur coordination et leur intégration au sein des différentes équipes.

Le deuxième facteur, les matières, fait référence aux ressources essentielles à la réalisation du projet. Cela inclut les matières premières, la qualité et la quantité des matériaux utilisés, ainsi que des éléments immatériels comme l'électricité, l'eau, les outils numériques ou encore l'accès à l'information.

Ensuite, le matériel et les machines regroupent les équipements indispensables au bon déroulement du projet. Cela peut inclure des machines industrielles, des moyens de transport, des outils informatiques et de communication comme les imprimantes, photocopieurs et téléphones. Ces investissements matériels jouent un rôle crucial dans l'efficacité des opérations.

Le quatrième élément, les méthodes, désigne l'ensemble des procédures, stratégies et modes d'organisation qui régissent la gestion des tâches et la mise en œuvre des activités. Il s'agit des démarches structurées, des objectifs stratégiques à atteindre, des plannings établis ainsi que des cadres politiques et culturels à respecter pour garantir une exécution optimale du projet.

Enfin, le milieu correspond à l'environnement global dans lequel évolue le projet. Il inclut des facteurs externes tels que les conditions climatiques, la localisation géographique, la dynamique du marché, la concurrence et les contraintes légales ou socioéconomiques. Pour approfondir cette analyse environnementale, l'outil PESTEL est souvent privilégié, permettant d'évaluer les influences politiques, économiques, sociales, technologiques, écologiques et légales susceptibles d'impacter la réussite du projet.

Cette structuration méthodique des cinq M facilite la compréhension des causes potentielles influençant un projet, aidant ainsi à mieux anticiper les risques et à adopter des solutions adaptées.

#### **1) L'Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (AMDEC)**

L'AMDEC (Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité) est une approche méthodologique qui permet d'anticiper et prévenir les dysfonctionnements possibles au sein d'un système, d'un processus ou d'un produit. En identifiant les points faibles et en évaluant leur impact, cette méthode aide à mettre en place des actions correctives et préventives pour améliorer la fiabilité et la sécurité des projets étudiés.

Connue sous l'acronyme FMECA en anglais (*Failure Mode, Effects and Criticality Analysis*), elle constitue un outil essentiel pour optimiser la gestion des risques et assurer une meilleure performance globale (Normalisation, 1986)

« Pour pouvoir effectuer une telle analyse, les spécifications du produit ou du processus doivent être établies. L'AMDEC peut identifier les domaines où des mesures préventives supplémentaires peuvent être appropriées pour minimiser les risques. » (ICH, 2005)

L'Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (AMDEC) est une approche inductive qui permet d'évaluer la fiabilité et la sécurité d'un système, tant sur le

plan qualitatif que quantitatif. Selon l'Association Française de Normalisation (AFNOR), cette méthode est principalement utilisée comme un outil d'analyse préventive, intervenant dès les phases de conception et d'industrialisation.

En tant que méthode prédictive, l'AMDEC vise à identifier les causes potentielles d'une défaillance ainsi que ses conséquences sur le fonctionnement global du procédé ou du moyen de production. Grâce à cette analyse approfondie, il devient possible de mettre en place des actions correctives ou préventives visant à réduire les risques et à optimiser la performance du système étudié. Cette approche proactive contribue ainsi à renforcer la qualité, la sécurité et la fiabilité des processus industriels.

## **2. Approches hybrides et innovantes de gestion des risques**

### **a) Cadres hybrides de gestion des risques**

Le cadre conceptuel est un choix populaire pour gérer les risques dans un environnement d'entreprise numérisé.

(Secureframe, 2024) Développé par le National Institute of Standards and Technology (NIST), le Risk Management Framework (RMF) est une approche structurée, flexible et mesurable, composée de sept étapes clés. Son objectif est d'intégrer les activités de sécurité et de gestion des risques dès les premières phases du cycle de vie du développement des systèmes, garantissant ainsi une protection proactive des actifs numériques. Ce cadre méthodologique veille à ce que la sécurité de l'information et la gestion des risques ne soient pas traitées comme des éléments secondaires, mais comme des piliers fondamentaux de la stratégie globale et des processus opérationnels de l'organisation.

### **1. Les avantages de la mise en œuvre du NIST RMF**

La mise en œuvre du Risk Management Framework (RMF), développé par le National Institute of Standards and Technology (NIST), apporte des avantages significatifs aux organisations souhaitant renforcer la sécurité et la gestion des risques au sein de leurs systèmes d'information.

Tout d'abord, le RMF permet une standardisation efficace des pratiques, assurant une gestion cohérente des risques à travers les différents départements et systèmes, tout en restant aligné sur les objectifs stratégiques de l'organisation. En outre, il garantit la conformité aux réglementations essentielles, notamment la Federal Information Security Modernization Act

(FISMA) de 2014, la Privacy Act de 1974, ainsi que les politiques de l'Office of Management and Budget (OMB) et les normes fédérales de traitement de l'information.

Un autre avantage clé réside dans l'intégration des protections de sécurité et de la vie privée à chaque phase du cycle de vie du développement des systèmes, permettant une gestion proactive des risques et une réponse adaptée aux menaces émergentes. Cette approche favorise une surveillance continue et une attitude préventive, essentielle pour anticiper les défis liés à la cybersécurité et à la protection des données.

Par ailleurs, le RMF facilite la prise de décision basée sur les risques, en fournissant un cadre structuré permettant aux organisations d'optimiser l'allocation des ressources et de mettre en œuvre des stratégies efficaces d'atténuation des menaces. Enfin, la flexibilité du RMF encourage une gestion des risques adaptée, où les contrôles sont ajustés en fonction du contexte organisationnel, garantissant ainsi leur pertinence et leur efficacité.

## **2. Etapes du cadre de gestion des risques de la NIST**

Le Risk Management Framework (RMF) du NIST repose sur sept étapes clés, conçues pour assurer une gestion efficace des risques dans les systèmes d'information. Ces étapes ne sont pas strictement linéaires et peuvent être adaptées selon les besoins organisationnels. Voici leur réinterprétation sous une forme plus fluide et humanisée :

### **Préparer**

Avant de gérer les risques, il est essentiel de définir un cadre clair et d'établir les priorités. Cette phase permet à l'organisation de structurer son approche, en attribuant des rôles et responsabilités, en évaluant les risques existants, et en mettant en place une stratégie de surveillance continue.

### **Catégoriser**

Chaque système d'information présente des vulnérabilités spécifiques. Cette étape consiste à identifier la criticité des données qu'il traite (confidentialité, intégrité, disponibilité) et à lui assigner un niveau de risque (faible, modéré ou élevé) afin d'adapter les mesures de protection.

### **Sélectionner**

Une fois la classification réalisée, il faut choisir les contrôles de sécurité appropriés. Ceux-ci sont définis selon les normes du NIST SP 800-53, puis ajustés en fonction des objectifs organisationnels, des menaces potentielles et des exigences réglementaires. Cette sélection doit également inclure une stratégie de surveillance à long terme.

### **Implémenter**

Les contrôles choisis sont ensuite mis en place dans l'environnement système. Cette étape nécessite une documentation claire expliquant comment chaque contrôle fonctionne, afin de garantir une application rigoureuse et efficace.

### **Evaluer**

Une fois les mesures de sécurité intégrées, il faut tester leur efficacité. Une équipe indépendante réalise des audits et évaluations, identifie les éventuelles failles et propose des ajustements pour renforcer la protection des données.

### **Autoriser**

Sur la base des résultats obtenus, l'organisation doit prendre une décision éclairée : le système peut-il être mis en service en l'état, ou nécessite-t-il des modifications ? Les décisions d'autorisation prennent en compte les risques résiduels et assurent une validation conforme aux exigences stratégiques et réglementaires.

### **Surveiller**

La gestion des risques ne s'arrête pas après la mise en service du système. Une veille continue permet de détecter les nouvelles menaces, d'évaluer l'évolution du niveau de risque et d'adapter les contrôles si nécessaire. La mise à jour de la documentation de sécurité garantit que l'organisation reste réactive face aux défis émergents.

Ce cadre assure une approche dynamique et proactive de la gestion des risques, permettant aux organisations de renforcer leur cybersécurité et leur conformité réglementaire.

**b) Six Sigma et Lean appliqués à la gestion des risques****• Six sigma**

Selon (shizen, 2023) Le Six Sigma représente une méthodologie stricte de gestion de la qualité, basée sur une approche statistique et mesurable pour l'amélioration des processus au sein d'une organisation. Cette approche, axée sur l'utilisation régulière de données quantifiables, a pour objectif d'atteindre une performance remarquable avec un taux de défaillance inférieur à 3,4 événements par million d'opportunités, ce qui équivaut à un niveau de qualité de 99,99966 %.

Le Six Sigma suit une approche organisée en cinq phases, connue sous le nom de DMAIC Définir, Mesurer, Analyser, Améliorer et Contrôler. D'après les partisans du Six Sigma, une entreprise peut venir à bout de tout problème apparemment insoluble en respectant ces cinq phases :

- Définir : Une équipe de personnes, dirigée par un expert du Six Sigma, choisit un processus à améliorer et définit le problème qu'elle souhaite résoudre.
- Mesurer : L'équipe mesure la performance initiale du processus, créant ainsi une référence, et identifie une liste d'entrées qui peuvent nuire à la performance.
- Analyser : Ensuite, l'équipe analyse le processus en isolant chaque entrée, ou cause potentielle de défauts, et en la testant comme cause racine du problème.
- Améliorer : L'équipe met en œuvre des changements qui vont améliorer la performance du processus.
- Contrôler : L'équipe ajoute des contrôles au processus pour s'assurer qu'il ne se dégrade pas et qu'il reste efficace.
- **Lean Management**

Selon (shizen, 2023) Lean Management constitue une méthodologie organisationnelle visant à maximiser la valeur perçue par le client tout en éliminant systématiquement les activités non productives. Son axiome central postule que toute ressource consommée - temps, matière ou effort - qui ne contribue pas directement à la création de valeur doit être considérée comme un gaspillage et, par conséquent, éliminée.

Les 5 principes fondamentaux pour construire un processus de gestion Lean efficace incluent : (Businessmap, s.d.)

Identifier la valeur : Déterminez ce dont les clients ont réellement besoin et éliminez le travail inutile.

Identifier la valeur : Déterminez ce dont les clients ont réellement besoin et éliminez le travail inutile.

Cartographier le Flux de Valeur : Visualisez comment le travail circule à travers le processus pour délivrer de la valeur.

Créer un Flux : Assurez-vous que le travail se déroule sans interruptions ni goulets d'étranglement.

Établir un système de tirage : Produisez uniquement ce qui est nécessaire, quand c'est nécessaire, pour éviter la surproduction.

Cherchez l'Amélioration Continue : Affinez continuellement les processus pour augmenter l'efficacité et l'adaptabilité.

Selon (shizen, 2023) Le Six Sigma et le Lean Management sont deux approches complémentaires qui, lorsqu'elles sont combinées, offrent des avantages significatifs pour l'amélioration des performances organisationnelles. Ensemble, elles permettent une meilleure compréhension des attentes et des besoins des clients, garantissant ainsi une approche centrée sur la satisfaction et la qualité. Cette synergie favorise également l'identification et l'élimination des sources de non-qualité, contribuant à une optimisation accrue des processus tant en termes d'efficacité que d'efficience. Par ailleurs, en impliquant activement les employés, cette approche améliore leur motivation et leur engagement, renforçant ainsi la culture de l'amélioration continue au sein de l'entreprise. Grâce à cette flexibilité, les organisations peuvent mieux s'adapter aux changements et saisir les opportunités qui se présentent, ce qui améliore leur compétitivité et leur rentabilité à long terme. Ainsi, l'intégration du Six Sigma et du Lean Management constitue un levier stratégique essentiel pour les entreprises souhaitant optimiser leur gestion et garantir une performance durable.

### c) **Management visuel des risques**

(Redsen, 2021), le management visuel, en tant que méthode issue du Lean Management, constitue un outil efficace pour l'optimisation des processus et l'amélioration de la collaboration au sein des organisations. Lorsqu'il est utilisé de manière pertinente, il permet une définition claire et précise des objectifs à atteindre, garantissant ainsi une meilleure orientation des actions et décisions. De plus, il favorise le partage d'une vision commune, ce qui contribue à une meilleure compréhension des enjeux et renforce l'alignement stratégique des équipes. Enfin, cette approche encourage une synergie entre les différents

acteurs, améliorant la coordination et la fluidité des échanges, tout en stimulant l'engagement et la performance collective. Grâce à ces atouts, le management visuel se présente comme une méthode fiable et bénéfique pour les entreprises souhaitant structurer efficacement leur gestion et leur prise de décision.

#### **d) Intelligence artificielle**

Selon (DIGITAL TPE, 2023) L'intelligence artificielle (IA) désigne la capacité des machines, en particulier des systèmes informatiques, à simuler des processus intellectuels humains tels que l'apprentissage, le raisonnement et l'auto-correction. Dans le domaine de la gestion des risques, l'IA joue un rôle clé en analysant d'importants volumes de données, permettant d'identifier des modèles et des tendances susceptibles d'anticiper des événements à risque. Grâce à ces analyses, les gestionnaires peuvent prendre des décisions plus éclairées et mettre en place des mesures proactives pour réduire les menaces potentielles.

L'IA trouve des applications variées en gestion des risques. Elle est notamment utilisée pour prévoir les risques financiers à travers l'analyse des tendances du marché et des données économiques, offrant ainsi la possibilité d'anticiper des crises ou des anomalies. Par ailleurs, elle facilite l'identification des risques opérationnels en surveillant les activités quotidiennes, détectant les anomalies et inefficacités pouvant perturber le fonctionnement des entreprises.

L'intégration de l'IA en gestion des risques offre de nombreux avantages. Elle améliore considérablement l'efficacité en automatisant les tâches de surveillance et d'analyse, libérant ainsi du temps pour des activités stratégiques. Son haut niveau de précision permet de traiter des quantités massives de données, conduisant à une meilleure identification des risques potentiels. Néanmoins, certains défis demeurent. La complexité des algorithmes exige une expertise avancée pour leur mise en œuvre et leur gestion. En outre, l'IA soulève des enjeux éthiques et de sécurité, notamment en matière de protection des données, de biais algorithmiques et de fiabilité des prédictions. Il est donc essentiel de prendre ces considérations en compte afin d'assurer une utilisation responsable et efficace de cette technologie.

#### **Conclusion du chapitre**

La gestion des risques apparaît comme un élément essentiel dans la conduite des projets, nécessitant une approche proactive et intégrée pour anticiper les menaces et saisir les

opportunités. Les outils et méthodes présentés dans la dernière partie offrent des solutions pragmatiques pour identifier, analyser et répondre efficacement aux risques, garantissant ainsi la pérennité et la performance du projet.

En combinant ces dimensions, ce travail contribue à une compréhension approfondie du management de projet et à une maîtrise efficace des risques.

**CHAPITRE 02 : MÉTHODOLOGIE DE  
LA RECHERCHE ET CONTEXTE  
ORGANISATIONE**

Dans ce chapitre, nous détaillerons la méthodologie retenue pour mener notre étude. Nous expliquerons le cadre épistémologique sur lequel nous nous appuyons, ainsi que les méthodes utilisées pour collecter et analyser les données, afin de répondre aux objectifs fixés.

### **Section 1 : Méthodologie de la recherche**

Dans cette section, nous présentons la méthodologie de notre recherche. Nous commençons par discuter du cadrage du projet, puis nous expliquons en détail la méthodologie d'enquête que nous avons adoptée. Nous abordons également les différentes méthodes de collecte de données utilisées, ainsi que les outils de collecte et de traitement des données.

#### **1. Cadrage du projet**

Pour cerner le périmètre de l'étude et déterminer les objectifs associés à l'analyse.

D'une part l'objectif de l'étude est de savoir comment améliorer les pratiques de gestion des risques de projet à travers des outils et des méthodes dans les processus de gestion de projet (démarrage du projet, planification, exécution, suivi et contrôle, et clôture du projet), d'autre part, il s'agit de la prise de décision tout au long du processus de gestion des risques du projet.

#### **2. Positionnement épistémologique de la recherche**

D'après Florence Allard-Poesie « Tout travail de recherche repose sur une certaine vision du monde, utilise une méthodologie, et propose des résultats visant à prédire, prescrire, comprendre ou expliquer », Ce qui souligne l'importance d'une épistémologie cohérente avec la recherche menée.

Avant d'aborder notre propre positionnement, il convient de rappeler en quoi consiste l'épistémologie et quel est son rôle. Selon (ZARDET & SAVALL, 1996) elle est définie comme « la théorie de la connaissance et de sa validité, il s'agit donc de l'étude critique des sciences, destinée à déterminer leur origine, leur valeur et leur portée ». Elle incite ainsi le chercheur à clarifier et exposer les paradigmes sur lesquels s'appuie sa recherche scientifique.

Cela conduit naturellement le chercheur à définir son positionnement paradigmatique. La littérature en sciences de l'organisation identifie principalement plusieurs cadres comme le constructivisme et le Positivisme.

Puisque notre recherche s'inscrit dans le cadre des sciences de gestion et risques dans le domaine IT, nous nous sommes donc orientés vers une posture épistémologique Pragmatisme, qui servent de référentiels fondamentaux aux travaux de recherche.

Présentation de la méthodologie de recherche : une recherche qualitative basée sur l'enquête. La méthodologie qualitative adopté dans cette recherche permet une exploration inductive de la manière dont les stratégies de gestion des risques sont conceptualisées, mises en œuvre et affinées dans le cadre de projets informatiques bancaires

Cette étude utilise une approche de recherche qualitative, qui cherche fondamentalement à étudier et à interpréter les significations complexes, les expériences vécues et les interprétations subjectives d'individus ou de collectifs dans des contextes sociaux particuliers. En tant que méthodologie interprétative la recherche qualitative utilise de multiples formes de matériel empirique, notamment des entretiens approfondis, des observations participantes, l'analyse de documents et du matériel visuel, ce qui permet une compréhension globale des phénomènes tels qu'ils sont construits et vécus par les acteurs sociaux dans leur environnement naturel. Cette orientation méthodologique est particulièrement utile pour saisir les perspectives nuancées et les facteurs contextuels qui façonnent les pratiques professionnelles dans les environnements organisationnels. ( Wendy & Kohn, 2014).

Par contre Dans le cadre d'une démarche de recherche, l'approche quantitative joue un rôle essentiel dans la validation et la démonstration des faits en s'appuyant sur la quantification des phénomènes étudiés. Cette méthode repose principalement sur la collecte de données à travers des outils tels que les questionnaires ou les sondages réalisés auprès d'un échantillon représentatif.

Les informations recueillies sont ensuite analysées sous forme de données statistiques, ce qui permet d'obtenir des résultats mesurables et objectifs. Ces données sont souvent présentées à l'aide de graphiques ou de tableaux, facilitant ainsi leur interprétation et leur mise en perspective dans le cadre de l'étude. ( Claude., 2019)

“répondre aux questions qui ont été soulevées, résoudre les problèmes qui ont été posés ou observés, évaluer les besoins et fixer des objectifs, déterminer si des objectifs spécifiques ont été atteints ou non, établir des bases de référence par rapport auxquelles des comparaisons futures peuvent être faites, analyser les tendances au fil du temps et, de

manière générale, décrire ce qui existe, en quelle quantité et dans quel contexte.” (Isaac & Michael , 1997).

La principale approche méthodologique adoptée est l'enquête. L'enquête est constamment appliquée pour construire des modèles théoriques en gestion des risques de projet, (da-Silvaa & António , 2014), basé sur une collecte de données qualitatives.

### **3. Les méthodes de collecte de données**

Aux fins de cette étude, des données qualitatives sont collectées pour permettre de répondre à notre problématique et à nos objectifs de recherche. Ces données sont collectées à différents moments de la démarche management des risques :

#### **a) L'observation**

La collecte de données par observation est une méthode où le chercheur examine directement, sur une période définie, les processus et comportements au sein d'une organisation. Cette approche permet d'obtenir des informations concrètes et vérifiables, évitant ainsi les biais d'interprétation souvent associés aux données verbales. En observant les événements tels qu'ils se déroulent, le chercheur s'assure d'une analyse fondée sur des faits réels, offrant une meilleure fiabilité aux résultats obtenus. ( Thietart, 2017)

#### **b) Brainstorming**

« Une méthode de créativité permettant de produire un maximum d'idées sur un thème donné » (Ernoul, 2010).

Afin d'identifier les mesures d'amélioration nécessaires à la planification de la gestion des risques et d'évaluer les risques internes et externes, des séances de réflexion ont été organisées avec les parties prenantes au processus de gestion des risques, ainsi que leurs besoins et leurs attentes. Chaque participant a apporté sa contribution en fonction de son expertise et de son expérience.

#### **c) L'entretien**

L'entretien est une méthode de collecte de données qui permet de recueillir des informations verbales en vue d'une analyse approfondie. Son principal intérêt réside dans sa capacité à explorer à la fois les pensées conscientes et les sentiments parfois refoulés des individus. En créant un cadre d'échange bienveillant, cette technique facilite la levée des mécanismes de défense que les participants pourraient mobiliser pour se protéger du regard extérieur sur leurs comportements et leurs opinions.

On distingue généralement trois types d'entretiens, chacun adapté à des objectifs spécifiques :

1. L'entretien directif

Dans cette approche, l'enquêteur structure l'échange en posant des questions précises, souvent fermées, afin d'obtenir des réponses ciblées. Il guide activement la discussion, ce qui permet de recueillir des données standardisées et comparables.

2. L'entretien non-directif (ou ouvert)

À l'inverse, cette méthode donne une grande liberté à l'interviewé. L'enquêteur utilise principalement des questions ouvertes, encourageant la personne à s'exprimer librement sur son vécu, ses perceptions et ses émotions. Cette approche favorise l'émergence d'informations riches et spontanées.

3. L'entretien semi-directif

Entre les deux précédents, ce format hybride combine questions fermées (pour préciser certains points) et ouvertes (pour approfondir les réponses). L'intervieweur conserve une certaine maîtrise du cadre tout en laissant à l'interviewé la possibilité de développer ses idées. ( Thietart, 2017)

Dans notre recherche nous avons opté pour les entretiens semi-directifs avec différents acteurs impliqués dans l'entreprise.

- **Guide d'entretien**

Comme mentionné au paravent, nous allons aborder un guide d'entretien qui vise à approfondir notre recherche, structuré de manière à recueillir des informations pertinentes.

Ce guide est destiné aux professionnels et experts du domaine de IT, les questions de guide ont été conçues de la manière suivante :

Une première rubrique :

Questions générales : pour mieux comprendre le profil des participants.

Une deuxième rubrique :

Questions spécifiques sur les pratiques de gestion des risques en matière de IT : en mettant l'accent les choix méthodologiques, l'équilibre entre approches classiques et innovantes, et

l'évaluation de leur efficacité. Elle analyse la priorisation des risques critiques, la comparaison des outils traditionnels et émergents, ainsi que l'optimisation des processus par l'automatisation des tests et l'apprentissage des incidents passés.

- **Argumentation de choix d'échantillon**

Le choix de l'échantillon pour notre recherche s'est porté sur quatre employés de l'entreprise BEYN, où se déroule le stage. Cette décision a été guidée par les contraintes organisationnelles, notamment la taille de l'équipe de développement qui est composée uniquement de ces quatre individus. La similarité des réponses fournies par les développeurs a permis d'atteindre une saturation des données, ce qui signifie que l'échantillon était suffisamment représentatif pour permettre une analyse pertinente des risques de sécurité. Ainsi, même restreint, cet échantillon a été jugé adéquat pour les besoins de l'étude.

**Tableau 1:** Tableau des entretiens

Business unit	Poste	Jour d'entretien	Durée
Consulting	Chef de projet	02/05/2025	40 min
Consulting	Product Owner	03/05/2025	35 min
Consulting	Responsable qualité	03/05/2025	30 min

Source : Elaborer par nous

#### **4. Traitement des données**

Une fois les données collectées, un traitement méthodique et approfondi a été effectué. Nous avons mobilisé le logiciel NVivo 10 afin d'analyser qualitativement les informations recueillies, tandis que l'outil AMDEC a été utilisé pour l'évaluation et la gestion des risques identifiés. Cette approche a permis d'assurer une analyse précise et structurée des données.

- **NVIVO 10**

Nous avons choisi d'utiliser NVivo 10, un logiciel spécialisé dans l'analyse des données qualitatives. Cet outil offre des fonctionnalités avancées pour organiser, explorer et interpréter des données textuelles. Dans le cadre de cette étude, NVivo 10 sera principalement mobilisé pour réaliser une analyse statistique des textes et générer des nuages de mots. Cette méthode permettra d'identifier les termes les plus fréquemment évoqués par les participants, offrant ainsi une représentation visuelle des thématiques dominantes abordées lors des entretiens.

Ce nuage de mots met en évidence les thématiques centrales d'un discours ou d'un corpus de textes axé sur la gestion des projets et la réponse aux risques, notamment dans un contexte académique ou professionnel. Les mots les plus saillants — réponse, risques, projet, gestion, approches — suggèrent une forte concentration sur la manière de gérer les incertitudes et les aléas au sein de projets, en particulier ceux liés au secteur bancaire ou technologique. L'importance accordée aux méthodes, méthodologie, tests *et* outils révèle un intérêt marqué pour les techniques d'évaluation, de prévention et de traitement des risques. L'apparition de termes comme *agile*, *waterfall*, *hybride*, ou encore *frameworks* indique une exploration des différentes approches de gestion de projet, classiques comme innovantes. Enfin, des mots comme *analyse*, *développer*, *améliorer*, ou *techniques* témoignent d'un objectif global d'optimisation, de maîtrise et de professionnalisation des processus décisionnels dans des environnements critiques ou complexes.

- **AMDEC**

Nous concevons une matrice AMDEC afin d'identifier et d'évaluer les risques potentiels associés à la sécurité des plateformes numériques. Cette matrice se présente sous la forme d'un tableau structuré en plusieurs colonnes, permettant une analyse détaillée et une gestion efficace des risques détectés.

Cette matrice s'affiche sous forme de tableau à plusieurs colonnes, comme suit :

- Identification des opérations et activités : Cette section recense les différentes opérations liées à la réalisation de la plateforme numérique qui feront l'objet d'une analyse approfondie.
- Modes de défaillance : Cette catégorie permet de répertorier les risques et défaillances potentielles pour chaque activité

- Effet potentiel des défaillances : Elle analyse l'impact probable de chaque mode de défaillance sur le système, cherchant à répondre à la question « *Quels seraient les effets associés ?* ».
- Causes possibles : Cette section vise à identifier les origines potentielles de chaque défaillance, facilitant ainsi la mise en place d'actions préventives.
- Gravité de l'impact : Un système de cotation de 1 à 5 est utilisé pour évaluer la gravité des effets, allant d'un impact mineur (1) à une conséquence critique (5).
- Fréquence d'apparition : La probabilité d'occurrence de chaque mode de défaillance est également quantifiée sur une échelle de 1 (très rare) à 5 (très fréquent).
- Capacité de détection : L'aptitude à identifier ces défaillances est mesurée selon un indice allant de 1 (détection très efficace) à 5 (détection faible).
- Criticité du risque : Cette métrique est obtenue en multipliant la gravité, la fréquence et l'indice de détection ( $C = G \times F \times D$ ). Elle permet de hiérarchiser les risques et d'adapter les mesures correctives en conséquence.
- Plan d'action : Une série de mesures correctives et préventives est recommandée pour atténuer les risques et limiter leur impact sur la sécurité du système.
- Attribution des responsabilités : Chaque action est associée à une personne ou une équipe responsable de sa mise en œuvre.

**Tableau 2:** Scores d'évaluation de la gravité

	Gravité (G)	
Score	Intitulé	Définition
5	Très faible	Cela signifie que si le risque se matérialise, ses conséquences seront négligeables, et qu'il est peu probable qu'il se produise.
10	Faible	Risques faibles nécessitant un suivi de routine et une évaluation trimestrielle.
15	Modéré	Risques modérés qui peuvent être acceptés avec des plans d'action de réserve en cas de déclenchement.
20	Élevé	Risques importants nécessitant des stratégies d'atténuation robustes et un suivi mensuel.
25	Critique	Risques nécessitant une attention immédiate, une stratégie d'évitement ou de réduction active, et un suivi hebdomadaire.

Source : Document interne de l'entreprise

**Tableau 3:** Scores d'évaluation de la fréquence

	Fréquence (F)	
Score	Intitulé	Définition
1	Très rare	L'apparition n'a jamais eu lieu encore possible dans certaines conditions particulières
2	Rare	Apparition une fois par an dans les conditions normales d'utilisation
3	Probable	Apparaître une à deux fois par an dans des conditions normales d'utilisation
4	Fréquente	Parution mensuelle dans les conditions normales d'utilisation

Source : élaborer par nous

**Tableau 4:** Scores d'évaluation de la détection

	Détection (D)	
Score	Intitulé	Définition
1	Evidente	DéTECTABLE sans aucune mesure
2	Facilement détectable	Facilement détectable une fois les mesures prises
3	Détectable	Détectable une fois les mesures prises
4	Difficilement détectable	Difficile de prédire son apparence

Source : élaborer par nous

La cotation des critères d'estimation a permis de calculer l'indice de priorité de risque IPR (Risk Priority Number RPN en anglais), encore appelé indice de criticité C de la défaillance considérée par cette formule :  $C = G \times F \times D$

Ces tableaux proposent une grille de notation permettant d'évaluer trois éléments clés de l'analyse AMDEC : la détection, la fréquence et la gravité des défaillances. Ces critères jouent un rôle crucial dans l'identification, l'évaluation et la hiérarchisation des risques potentiels au sein d'un système ou d'un processus. En structurant ces données de manière méthodique, il devient plus facile de définir les priorités et de mettre en place des plans

d'action adaptés, visant à minimiser les risques et à renforcer la fiabilité ainsi que la sécurité des systèmes étudiés.

### **Conclusion de la section**

Notre méthodologie repose sur une approche qualitative, privilégiant une enquête approfondie pour explorer les défis liés à l'élaboration des solutions e-banking (plateformes numériques). Pour cela, nous avons mis en place une collecte de données basée sur des entretiens semi-directifs avec des experts du domaine et des observations directes des systèmes étudiés. Cette démarche nous permet d'obtenir des retours détaillés et nuancés, essentiels pour identifier les risques et proposer des recommandations adaptées. L'accent est mis sur l'outil AMDEC, dont l'efficacité est évaluée à travers les retours des participants et l'analyse des données recueillies. Cette méthodologie nous offre une vision globale et pragmatique de la gestion des risques dans les environnements numériques.

## Section 2 : Contexte organisationnel

Cette section présente une analyse approfondie de l'organisme d'accueil, fondée sur nos observations directes et enrichie par l'expertise du manager ainsi que les informations disponibles sur le site officiel de l'entreprise. Cette démarche nous a permis de développer une vue d'ensemble complète et détaillée, garantissant une représentation fidèle de la structure, de son fonctionnement et de son environnement.

### 1. Présentation de l'entreprise

BEYN est une fintech algérienne spécialisée dans le développement de solutions numériques dédiées au secteur bancaire. Fondée en 2004, elle s'est imposée comme un acteur clé de la transformation digitale des services financiers en Algérie. Son expertise couvre notamment la conception de plateformes d'e-banking, de solutions de paiement mobile et d'outils innovants visant à optimiser l'expérience utilisateur et la sécurité des transactions.

Avec plus de 15 ans d'expérience, BEYN a su développer des partenariats solides avec plus de dix banques algériennes, leur fournissant des solutions adaptées aux besoins des particuliers et des entreprises. Son approche repose sur une écoute active des clients, une agilité technologique et une capacité d'innovation constante, lui permettant de répondre aux défis du secteur bancaire numérique.

L'entreprise est également engagée dans le développement de solutions de paiement mobile, un domaine en pleine expansion en Algérie et à l'international. Grâce à son modèle économique innovant, BEYN attire l'intérêt de banques étrangères et continue d'élargir son influence sur le marché financier numérique.

### 2. Contact de l'entreprise

Son siège est situé à Cheraga, Wilaya d'Alger, et elle compte une équipe dynamique qui mise sur la formation continue et l'évolution professionnelle pour garantir des services de haute qualité.

- **Adresse** : Zone d'Activités Amara, Lot n°04, Bt G, Étage 03, Route d'Ouled Fayet, Chéraga, Alger.
- **Téléphone** : 023 30 59 12 / 023 35 39 20.
- **Email** : amina.baghdadi@beyn.io

### 3. Missions et Valeurs

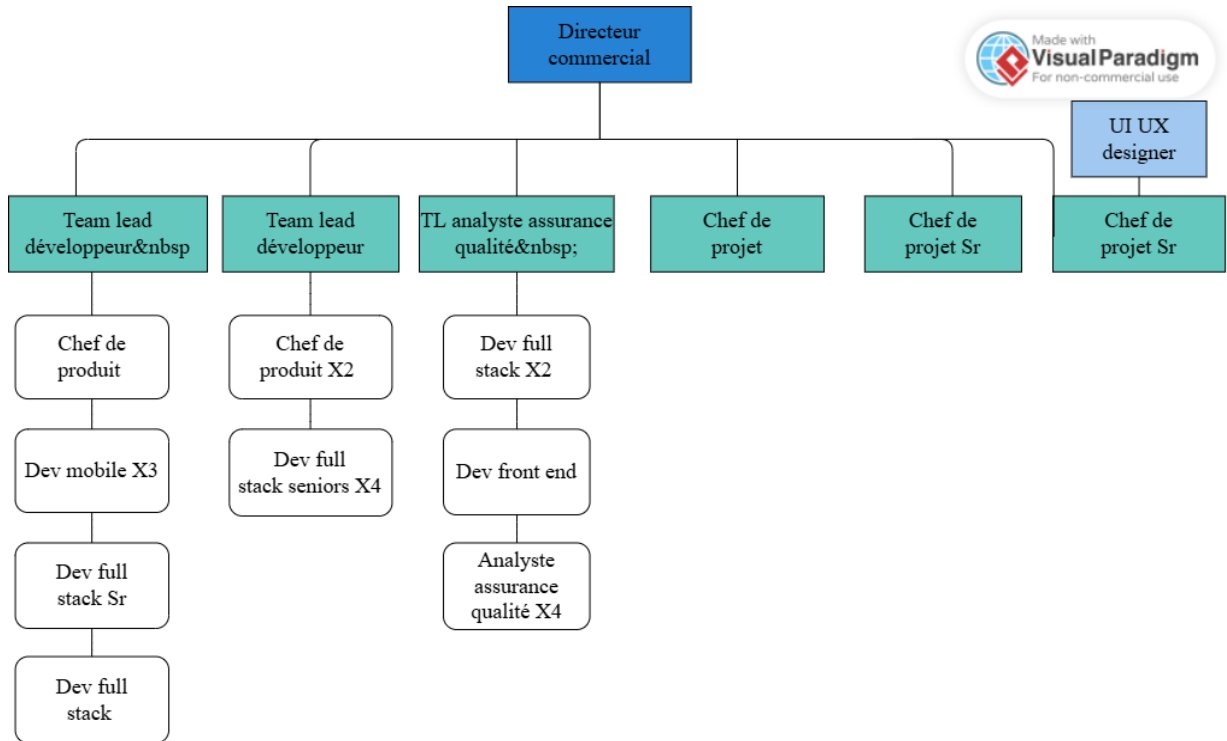
L'entreprise s'engage à jouer un rôle clé dans l'inclusion financière en développant des solutions digitales destinées aux établissements bancaires. Ces technologies visent à élargir l'accès aux services financiers, en modernisant les systèmes de paiement et en optimisant les processus bancaires pour les rendre plus efficaces et inclusifs. Au-delà de l'innovation technique, notre approche repose sur des valeurs fondamentales :

- **Focus client** : Nous plaçons la satisfaction de nos partenaires au cœur de notre action, en adoptant une démarche collaborative où chaque projet devient une réussite collective.
- **Connexion** : Notre expertise consiste à renforcer le lien entre les banques et leurs clients grâce à des outils digitaux accessibles en permanence, quel que soit le lieu où le moment.
- **Ambition** : Nous aspirons à démocratiser les services financiers en proposant des solutions intuitives, disponibles 24h/24 et adaptées à tous les canaux (agences, mobiles, tablettes, ordinateurs).
- **Inspiration** : Portées par une équipe jeune et créative, nos innovations répondent aux attentes des clients les plus exigeants, en intégrant les dernières avancées technologiques.
- **Engagement** : Nous accompagnons nos partenaires dans leur transformation digitale avec des solutions flexibles, évolutives et déployables rapidement, afin de s'adapter en temps réel aux besoins du marché.

#### 4. L’organigramme de l’entreprise

Cet organigramme représente la structure hiérarchique de BU PROJET.

**Figure 3:** organigramme de l’entreprise.



Source : document interne de l’entreprise

#### 5. Gamme des produits

SELA :

SELA est une plateforme de Digital Banking omnicanale et multi-device, conforme DSP2, qui offre une expérience fluide.

Facilement intégrable aux systèmes existants, elle permet un déploiement rapide. Son approche modulaire s’adapte à votre stratégie et à votre marché. SELA améliore l’efficacité commerciale grâce à une vision client à 360°.

KANTARA :

KANTARA est une solution digitale de nouvelle génération facilitant la gestion de trésorerie des petites, moyennes et grandes entreprises. Elle centralise les flux via un accès unique et permet un pilotage simple, en temps réel. La plateforme s’intègre aux systèmes internes et gère plusieurs entités, devises ou pays.

Kantara s'adapte aux organisations des clients entreprises grâce à une gestion fine des pouvoirs & habilitation.

WIMPAY :

Wimpay payeur est une solution de paiement mobile instantanée, simple et sécurisée.

Elle permet à l'utilisateur de payer ses achats, envoyer et recevoir de l'argent sans cash.

Fonctionnalités :

Paiement marchand (QR code)

Transferts de personne à personne (PtoP)

Gestion des contacts & des favoris

Wimpay marchand est une solution d'acceptation sécurisée permettant au marchand de percevoir leur paiement et de gérer leurs points de vente.

Fonctionnalités :

Acceptation en magasin par QR Code

Remboursement

Gestion des points de ventes

Reporting

### **6. La structure organisationnelle**

**La Business Unit Édition :** se concentre sur la conception de produits en marque « blanche ». Ces programmes sont conçus pour être modulables selon l'identité visuelle et les besoins spécifiques des clients, tout en conservant leurs fonctionnalités principales. Un logiciel en marque blanche est, dans les faits, une solution standard adaptable et personnalisable selon les exigences du client, lui offrant ainsi la chance de le commercialiser sous sa propre marque. Après cela, ces produits sont commercialisés selon le modèle SaaS.

**L'équipe BU Partenaires :** est responsable de tous les produits SAAS et répond aux exigences spécifiques des clients concernant ces solutions. Cette équipe est responsable de la surveillance et de l'amélioration des plateformes en place.

**La Business Unit Consulting,** une équipe spécialisée dans le conseil et la gestion de projets complexes. Cette BU intervient exclusivement sur des missions obtenues par voie d'appels

d'offres publics ou de consultations restreintes, ce qui lui confère une expertise particulière dans le cadre réglementaire des marchés publics et privés.

Son cœur de métier consiste à prendre en charge l'intégralité du cycle projet pour des solutions sur-mesure : depuis l'analyse des besoins clients jusqu'à la livraison finale, en passant par la conception et la mise en œuvre. Cette approche globale permet d'apporter des réponses adaptées aux enjeux spécifiques de chaque partenaire institutionnel ou entreprise.

La BU Consulting se distingue ainsi par :

- Son savoir-faire dans les processus d'acquisition compétitifs
- Sa capacité à gérer des projets clés en main
- Son expertise en personnalisation de solutions
- Son approche rigoureuse du cadre contractuel

Le stage s'est déroulé au sein de la BU Consulting donc :

### **a) Mission de la structure BU Consulting**

Projet BU repose sur une approche globale visant à concevoir et développer des solutions applicatives sur mesure (web & mobile), tout en garantissant leur qualité, sécurité et performance. L'intégration de solutions de paiement et d'authentification constitue un axe clé, assurant une interopérabilité fluide avec les systèmes existants. Afin de garantir la pérennité des projets, un support complet est mis en place tout au long du cycle de vie, accompagné d'une maintenance applicative proactive pour assurer le bon fonctionnement et l'optimisation des solutions en production.

### **b) Projets réalisés par l'entreprise**

Face à la numérisation rapide du secteur bancaire, la Banque AGB (Algerian Gulf Bank) a lancé une initiative stratégique pour actualiser ses services numériques, améliorer sa relation avec les clients et offrir une expérience utilisateur avant-gardiste à tous ses clients, qu'ils soient particuliers ou entreprises. Reconnaisant les transformations majeures des pratiques bancaires, AGB a reconnu l'impératif de réviser son canal numérique par le biais d'une révision intégrale de son système de banque en ligne.

dans ce contexte que l'entreprise BEYN a été choisie pour la création de la nouvelle plateforme d'e-banking d'AGB. La proposition de BEYN s'est démarquée grâce à sa connaissance approfondie des technologies bancaires, l'étendue des fonctionnalités de sa solution et son aptitude à personnaliser le produit en fonction des exigences métiers spécifiques d'AGB.

Le projet a été présenté dans le cadre d'une consultation restreinte, visant des fournisseurs reconnus pour leur compétence en matière de banque numérique et de sécurité bancaire.

### **Périmètre fonctionnel du projet**

Le périmètre du projet couvre à la fois la migration des données de l'e-banking existant et le développement de fonctionnalités réparties en deux lots principaux :

Le Lot 1 inclut les fonctionnalités essentielles à une première mise en production rapide et efficace :

- L'espace public pour la communication institutionnelle et l'accès aux simulateurs de produits,
- La consultation des comptes,
- La gestion des cartes,
- La réalisation de virements,
- La gestion des notifications,
- Les modules de pré-domiciliation et domiciliation,
- Et certains services bancaires en ligne tels que les demandes de chéquier, les réclamations, et les alertes SMS.

Le Lot 2 vise à enrichir la solution avec des services avancés, notamment :

- Le module de gestion des crédits (consultation, simulation, et demande),
- Le module de commerce extérieur, incluant la gestion des remises documentaires et lettres de crédit,
- L'onboarding digital pour la souscription à distance,

-Ainsi que le module multi-langue afin de rendre la plateforme accessible à une audience plus large.

Ce découpage par lots permet de respecter les délais de livraison tout en garantissant une montée en charge progressive et maîtrisée. En parallèle au développement fonctionnel, une attention particulière est portée à la migration des données, en s'appuyant sur des API exposées par le core banking pour synchroniser en temps réel les données de soldes, virements et transactions.

### **Conclusion du chapitre**

Ce chapitre a présenté l'organisation interne de BEYN ainsi que la méthodologie adoptée pour analyser les risques liés à la réalisation des plateformes numériques bancaires. Il a mis en avant l'importance de comprendre la structure et les processus internes afin d'identifier et de gérer efficacement les vulnérabilités susceptibles d'impacter les services financiers digitaux. En explorant diverses approches de recherche et d'analyse, cette étude a permis de poser les bases d'une évaluation approfondie des risques, ouvrant ainsi la voie aux discussions et recommandations stratégiques qui seront développées dans les sections suivantes.

# **CHAPITRE 03 : RÉSULTATS ET DISCUSSION**

Ce chapitre expose les résultats de notre étude en mettant en avant deux aspects fondamentaux. Il joue un rôle clé dans l'interprétation des conclusions de notre recherche et leur application concrète au sein de l'entreprise **BEYN**.

## **Section 1 : résultats de l'étude qualitative**

### **1. Déroulement de l'observation :**

Au cours de mon stage final, j'ai eu l'opportunité de rejoindre une fintech algérienne qui se consacre au développement de logiciels et plateformes dédiés à la banque. Cette entreprise se démarque par sa faculté à offrir deux schémas économiques complémentaires pour satisfaire les exigences diverses du domaine bancaire.

Cette expérience basée sur les brainstormings nous a permis d'observer le processus de création de sites web et d'applications, tout en acquérant des compétences d'identification et d'évaluation des risques liés au secteur e-banking.

### **2. Déroulement des entretiens**

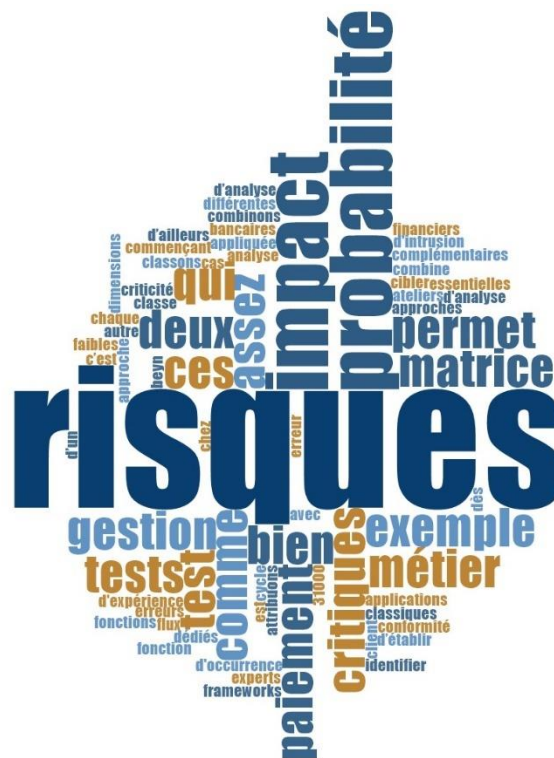
Dans le cadre de la mise en place d'une matrice AMDEC pour le développement de logiciels et de plateformes bancaires, nous avons mené trois entretiens avec des experts du domaine. L'objectif était d'identifier les risques potentiels liés à chaque phase du développement, tout en prenant en compte les exigences réglementaires et normatives applicables au secteur financier.

Ces échanges ont joué un rôle essentiel dans la collecte d'informations stratégiques, nous permettant de mieux comprendre les vulnérabilités susceptibles d'affecter la fiabilité et la sécurité des solutions bancaires numériques. Nous avons ainsi pu cartographier les risques majeurs associés aux différentes étapes de conception, de test et de déploiement des logiciels, tout en analysant les mesures préventives existantes et en définissant des actions correctives adaptées pour renforcer la résilience des systèmes.



Selon le MP« L'approche de gestion des risques varie en fonction de la méthodologie employée. Dans la méthode Waterfall, nous mettons en place un registre des risques dès le début, avec des examens prévus à des jalons cruciaux. Dans le cadre Agile, nous incorporons cet aspect lors des cérémonies périodiques telles que les planifications de sprint et les rétrospectives, favorisant une détection et un ajustement constant. Dans notre stratégie hybride, nous associons une analyse préliminaire détaillée à des révisions régulières tout au long du processus de développement. Quoi qu'il en soit, nous nous basons sur une matrice de criticité pour hiérarchiser nos actions et assurons une communication claire avec nos clients du secteur bancaire concernant les risques détectés. »

**Figure 5:** nuage de mots d'axe 02 les Approches classiques de gestion des risques



Source : générer par NVIVO 10

La convergence entre l'analyse théorique et les pratiques terrain met en exergue la rigueur méthodologique qui caractérise la gestion des risques dans le secteur bancaire, notamment dans les projets IT sensibles comme les applications de paiement. L'utilisation systématique de la matrice de criticité « Nous utilisons une matrice de criticité basée sur deux axes : l'impact (financier, réputationnel, réglementaire, utilisateur) et la probabilité d'occurrence. Un bug mineur sera par exemple classé comme faible (impact limité, occurrence faible),

tandis qu'un risque de fraude ou une faille de sécurité sera automatiquement classé critique, en raison de son impact potentiel sur la confiance des utilisateurs et la conformité légale. Chaque risque critique fait l'objet d'un suivi renforcé avec des plans de contingence définis et testés. PO », fondée sur une évaluation croisée de l'impact — qu'il soit financier, réputationnel, réglementaire ou centré sur l'utilisateur — et de la probabilité d'occurrence, permet une hiérarchisation objective des risques. Cette approche, typique des méthodes traditionnelles, est renforcée par des outils éprouvés tels que les tests d'intrusion, les analyses sectorielles et les retours d'expérience. Elle s'inscrit dans un processus global d'intégration des risques aux opérations métiers, rendant leur gestion à la fois conforme aux normes réglementaires et alignée avec les enjeux métiers. En parallèle, le recours aux experts métiers et sécurité rappelle le poids fondamental de l'expertise humaine dans l'appréciation de menaces complexes ou non quantifiables. L'ensemble souligne une synergie entre méthode structurée, outils technologiques, et intelligence collective, garantissant une couverture robuste des vulnérabilités critiques.

**Figure 6:** nuage de mots d'axe 03 sur les Approches innovantes et Amélioration continue



Source : générer par NVIVO 10

Ce croisement entre les mots-clés du nuage et les témoignages professionnels et du tableau d'observation révèle une application concrète et performante des approches innovantes dans la gestion des risques. L'importance accordée aux termes tels que « tests », « détection », « développement » ou encore « validation » traduit une logique centrée sur l'anticipation des défaillances et l'optimisation continue des processus. Cette dynamique se retrouve dans les pratiques décrites, où chaque incident devient une opportunité d'apprentissage structuré à travers des retours d'expérience formalisés et des actions préventives ciblées. L'usage d'indicateurs comparatifs permet d'évaluer objectivement l'efficacité des nouvelles pratiques, qui, par le biais de méthodes agiles ou d'automatisation des tests, favorisent une détection précoce des anomalies, une meilleure réactivité des équipes et une plus grande stabilité des livrables. La réduction des bugs critiques et l'élévation du niveau de satisfaction client témoignent de l'impact tangible de ces méthodes, ancrant l'innovation dans une logique de résultats mesurables et durables.

### **3. La mise en place de l'AMDEC**

#### **Étape 01 : constitution de l'équipe de travail**

L'équipe chargée de cette analyse était composée de

- Benyoucef Dhouha
- Chef de projet AGB
- Product Owner de projet

Le but de l'étude était d'analyser les risques relatifs au processus de et d'élaborer une matrice d'AMDEC au niveau de l'entreprise BEYN

#### **Étape 2 : étude fonctionnelle**

Dans le cadre de notre recherche, nous avons mené une étude qualitative portant sur les risques liés à la modernisation et optimisation de canal numérique de banque. L'objectif était d'identifier les défaillances potentielles susceptibles d'affecter leur fiabilité et leur résilience.

Pour cela, nous avons adopté une approche méthodologique rigoureuse, combinant plusieurs sources d'information afin d'obtenir une vision globale des menaces existantes. Une série

d'entretiens semi-directifs a été réalisée auprès de divers acteurs économiques de l'entreprise, notamment les responsables et chefs de projets. Ces échanges ont permis de recueillir des données essentielles sur les vulnérabilités identifiées, les mécanismes de prévention existants et les stratégies à renforcer pour une meilleure gestion des risques.

Les risques identifiés sont :

- **Techniques** : Relatifs aux défis techniques de développement, d'intégration et de compatibilité.
- **Sécurité et Conformité** : Liés à la protection des données, à la conformité réglementaire, et à la cybersécurité.
- **Organisationnels et Humains** : Concernent la gestion des équipes, la disponibilité des ressources et la communication inter-équipes.
- **Financiers** : Liés aux contraintes budgétaires et aux imprévus financiers.
- **Délais et Calendrier** : Concerne le respect des jalons et des délais de livraison.
- **Externes** : Inclut les risques de pandémie, les perturbations des fournisseurs, et d'autres événements externes pouvant affecter le projet.

### Étape 3 : étude qualitative des défaillances

Nous avons mené une analyse qualitative des défaillances potentielles. L'objectif était d'identifier les vulnérabilités susceptibles de se manifester à chaque phase de l'opération. Pour cela, nous avons effectué un examen approfondi de chaque étape, en déterminant les causes possibles des défaillances ainsi que leurs impacts sur l'entreprise et ses clients. Cette approche nous a permis de mieux comprendre les risques et d'anticiper les mesures correctives adaptées pour assurer la fiabilité et la performance du processus.

Ensuite, nous avons effectué une observation directe du processus de réalisation de platform. Cela nous a permis de détecter des défaillances potentielles qui pourraient ne pas avoir été identifiées lors des entretiens. L'observation nous a également permis de comprendre davantage le déroulement du processus et d'analyser les points critiques.

**Étape 4** : étude quantitative des défaillances

Une fois les modes de défaillances identifiés, nous sommes passés à leur évaluation. Pour cela, nous avons estimé la criticité de chaque défaillance identifiée en se basant sur les critères présentés dans le chapitre précédent.

**Étape 5** : la hiérarchisation

Après avoir déterminé la criticité de chaque mode de défaillance, il était essentiel de procéder à leur classification afin d'identifier celles nécessitant des actions correctives où. Les critères d'évaluation ont été établis sur la base des échelles proposées par le consultant en systèmes de management et ont été validés après une discussion approfondie avec l'équipe. Cette démarche visait à garantir une évaluation objective et quantifiée de chaque risque, facilitant ainsi la prise de décisions et l'élaboration de stratégies adaptées pour optimiser la gestion des défaillances.

En fonction des scores de criticité obtenus, nous avons donc défini une échelle de priorité :

**Tableau 5:** Échelle de priorité.

Niveau de risque évalué	Définition de risque	Acceptabilité
$5 \leq C \leq 40$	Risque acceptable	Risque tolérable ne nécessitant aucune action corrective.
$41 \leq C < 135$	Risque Modérer	Risque maîtrisé grâce aux mesures mises en place.
$136 \leq C \leq 320$	Risque indésirable	Risque inacceptable nécessitant une gestion à moyen terme.
$320 \leq C \leq 400$	Risque inacceptable	Risque critique nécessitant une intervention immédiate pour le maîtriser.

Source : élaborer par nous-mêmes

L'évaluation s'appuie sur une matrice à cinq niveaux qui mesure trois dimensions clés des risques : la gravité (de "Très faible" à "Critique", notée de 1 à 5), la fréquence (de "très rare" à "fréquent", notée de 1 à 4) et la capacité de détection (de "évident" à "difficilement

délectable", notée de 1 à 4). Cette méthodologie, conforme aux critères établis précédemment, permet une analyse complète et nuancée du profil de risque, facilitant ainsi la priorisation des actions de mitigation

**Étape 6** : La recherche des actions préventives/correctives

Dans le cadre de notre étude, nous avons mis en place des mesures préventives afin de limiter les risques, notamment ceux présentant une fréquence élevée ou une gravité importante. L'objectif était de réduire les probabilités de dysfonctionnement et d'atténuer les risques difficilement détectables.

Les actions correctives et préventives ont été élaborées en fonction du niveau de risque associé à chaque défaillance identifiée, en s'appuyant sur les propositions formulées par les développeurs lors des entretiens. Cette démarche collaborative a permis de mobiliser les expertises de chaque membre de l'équipe pour garantir des solutions adaptées et efficaces.

Les mesures recommandées ont été spécifiquement conçues pour cibler les causes potentielles des défaillances, renforçant ainsi la fiabilité et la sécurité des systèmes analysés. Cette approche proactive favorise une gestion optimale des risques, essentielle à l'amélioration continue des processus de développement.

**Étape 07** : le suivie et la réévaluation de la criticité

Dans le cadre de notre recherche, nous avons mis en place des mesures adaptées visant à atténuer les risques, en accordant une attention particulière à ceux présentant une fréquence élevée ou une gravité importante. L'objectif principal était de réduire les probabilités de défaillance et de renforcer la capacité de détection des anomalies.

Afin d'optimiser cette démarche, nous avons mené une série d'entretiens approfondis avec l'ensemble des développeurs, ce qui nous a permis d'élaborer des solutions correctives et préventives proportionnelles au niveau de risque identifié pour chaque anomalie. Cette approche collaborative a favorisé la mobilisation des compétences et des expertises au sein de l'équipe, garantissant ainsi des décisions pertinentes et adaptées aux enjeux du projet.

Les mesures préconisées ont été spécifiquement conçues pour cibler les causes profondes des défaillances identifiées, dans le but d'améliorer la fiabilité des systèmes et d'assurer une

gestion proactive des risques. Cette méthodologie s'inscrit dans une logique d'amélioration continue et de sécurisation des processus en place.

### Étape 08 : la présentation des résultats

Les résultats de notre étude ont ensuite été présentés dans le tableau type AMDEC :

Tableau AMDEC (Annexe 05)

Dans le cadre de notre projet visant à mettre en place la matrice AMDEC dans le processus de production de l'entreprise BEYN, nous avons réussi à identifier les éléments suivants :

- ✓ Nous avons identifié 22 modes de défaillance, chacun ayant des effets indésirables.
- ✓ Nous avons identifié 43 causes potentielles qui peuvent affecter ces modes de défaillance.
- ✓ Nous avons recensé 22 techniques de contrôle pour détecter ces défaillances.

Grâce à ces trois analyses, nous avons pu calculer et évaluer la criticité (IPR) de chaque mode de défaillance.

En conclusion, nous avons identifié :

**Tableau 6:** Classification de l'acceptabilité des risques

12 Risques acceptable	
2 Risque Modérer	
1 Risques indésirable	
3 Risques inacceptable	

Source : Elaboré par nous

Après avoir analysé la criticité de chaque mode de défaillance, nous avons élaboré des plans d'action ciblés, en désignant les responsables chargés de leur mise en œuvre. Au total, dix recommandations ont été formulées, combinant des mesures préventives et correctives afin de limiter l'impact des risques identifiés et d'anticiper les éventuelles anomalies.

Ces recommandations ont été définies lors de la création de la matrice AMDEC le 5 mai 2025, en tenant compte des exigences et des contraintes du processus étudié.

Évaluation de l'efficacité du plan d'actions :

Le tableau ci-dessous présente une analyse comparative de la classification des risques en fonction de leur criticité, avant et après la mise en œuvre du plan d'actions.

**Tableau 7:** analyse comparative des criticités.

Criticité	Avant le plan	Après le plan
Risque acceptable	5	0
Risque Modérer	3	1
Risque indésirable	2	1
Risque inacceptable	0	0

Source : Elaboré par nous

L'évaluation des risques avant et après la mise en œuvre du plan d'action montre des améliorations notables dans leur gestion. Les risques acceptables ont été totalement éliminés, tandis que les risques modérés ont diminué, passant de 3 à 1, indiquant l'efficacité des mesures mises en place. La réduction des risques indésirables, de 2 à 1, souligne une avancée progressive, bien qu'un suivi reste nécessaire. Enfin, l'absence de risques inacceptables confirme une gestion maîtrisée des menaces les plus critiques dès le départ. Ces résultats mettent en lumière l'impact positif des stratégies adoptées et l'importance d'un suivi constant pour garantir la fiabilité des systèmes.

## Section 2 : Discussion

Les résultats de notre étude, qui a appliqué la méthodologie AMDEC à la gestion des risques dans un environnement fintech, démontrent un fort alignement avec la littérature existante tout en offrant des perspectives pratiques pour le secteur de la banque en ligne. Mes résultats confirment bon nombre des cadres théoriques examinés dans la revue de la littérature, mais mettent également en évidence les domaines dans lesquels l'application dans le monde réel nécessite une adaptation et une innovation.

### 1. Alignement sur les cadres théoriques

Mes recherches ont permis d'identifier six catégories de risques clés - technique, sécurité/conformité, organisationnel/humain, financier, calendrier et externe - qui reflètent étroitement les classifications proposées par des chercheurs tels que (KHELIFA & DERRADJI, 2016) et (ALAOUI & DHIBA, 2022). L'accent mis sur les risques liés à la cybersécurité et à la conformité réglementaire dans mes conclusions soutient leur argument selon lequel la banque numérique introduit des vulnérabilités uniques, en particulier en ce qui concerne les opérations transfrontalières et la protection des données. Cela valide l'affirmation de la littérature selon laquelle les environnements de banque en ligne nécessitent des approches de gestion des risques spécialisées qui vont au-delà des modèles traditionnels.

La méthodologie AMDEC s'est avérée particulièrement efficace pour structurer le processus d'évaluation des risques, confirmant les observations de (Rodrigues-da-Silva & Crispim, 2014) sur l'importance de cadres adaptables. En décomposant l'analyse en phases claires - des entretiens qualitatifs à la notation quantitative - j'ai pu reproduire l'approche recommandée par ces auteurs, qui consiste à adapter la gestion des risques à la maturité de l'organisation. Notre utilisation des scores de criticité ( $5 \leq C \leq 40$  et  $320 \leq C \leq 400$ ) pour hiérarchiser les risques s'aligne également sur leur insistance sur l'évaluation dynamique, bien que notre étude ait ajouté de la valeur en testant ce système dans un véritable projet de fintech.

### 2. Contributions pratiques et divergences

Alors que la littérature a fourni une base théorique solide, notre application a révélé des défis pratiques qui sont moins soulignés dans les travaux académiques. Par exemple, la conduite

d'entretiens avec des développeurs et des chefs de projet a permis de mettre au jour des risques organisationnels nuancés - tels que les lacunes en matière de communication entre les équipes - que les modèles théoriques négligent souvent. Cette constatation appuie l'argument de (Mercier-Laurent, 2016) sur l'importance des facteurs humains et des connaissances dans la gestion des risques, mais ajoute des exemples concrets tirés du secteur de la fintech.

L'efficacité de la documentation statique est un domaine dans lequel mes résultats divergent de la littérature. Alors que (AFNOR, Gestion des risques projet IT, 2003) et d'autres auteurs critiquent les cadres rigides, notre étude a révélé que les modèles structurés (comme le tableau AMDEC) amélioreraient en fait la clarté lorsqu'ils étaient associés à des mises à jour itératives. Cela suggère que le problème ne réside pas dans la documentation elle-même, mais dans une mise en œuvre rigide - une nuance qui pourrait éclairer les recherches futures.

### **3. Comblant les lacunes de la littérature**

Le projet a directement comblé plusieurs lacunes identifiées dans l'analyse de la littérature. Tout d'abord, en me concentrant sur une étude de cas de fintech, j'ai fourni des données empiriques pour un secteur qui (Rodrigues-da-Silva & Crispim, 2014) a noté qu'il était sous-représenté dans les études sur la gestion des risques. Deuxièmement, la réduction réussie des risques de haute criticité (comme le montre le tableau 6) a démontré que les stratégies d'atténuation proactives peuvent fonctionner dans la pratique, et pas seulement en théorie, répondant ainsi à l'appel de (Claudiu, 2007) pour des cadres plus faciles à mettre en œuvre.

L'accent mis sur le suivi en temps réel tout au long du cycle de vie du projet a également apporté une solution à la préoccupation de (Le Coze, et al., 2020) concernant l'incapacité des modèles conventionnels à détecter les risques en cascade. En observant directement les processus et en mettant à jour les évaluations des risques en permanence, notre approche a permis une plus grande réactivité que les méthodes rétrospectives traditionnelles.

### **Conclusion**

Notre étude jette un pont entre la théorie et la pratique de la gestion des risques en validant les cadres académiques par une application dans le monde réel tout en proposant des améliorations basées sur l'expérience pratique. Les résultats confirment que les méthodologies structurées telles que l'AMDEC restent précieuses, mais qu'elles doivent être

flexibles pour répondre aux risques dynamiques de la banque numérique. Ces résultats s'inscrivent dans la ligne du thème principal de la littérature : l'évolution de la technologie s'accompagne d'une évolution de nos approches en matière de résilience et de sécurité des systèmes.

En fondant les théories académiques sur des cas concrets, ma recherche contribue à l'évolution permanente des stratégies de gestion des risques à l'ère de la fintech. Les travaux futurs devraient s'appuyer sur ces résultats pour développer des outils encore plus adaptables à notre paysage numérique de plus en plus complexe.

# **CONCLUSION GÉNÉRALE**

Dans cette étude, notre objectif principal était d'explorer la gestion des risques dans le cadre d'un projet IT, en nous concentrant sur le cas du projet AGB chez BEYN (ex-AeBS Algeria e-Banking Services). Nous avons cherché à identifier les risques critiques, à évaluer leur impact, et à proposer des outils et des méthodes pour les maîtriser efficacement, en mettant en avant l'Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (AMDEC) comme approche structurante.

Cette recherche s'est articulée autour de trois chapitres clés. Le premier chapitre a posé les bases théoriques en examinant la littérature sur la gestion des risques, les méthodologies de projet (prédictive, agile, hybride), et les outils d'analyse comme l'AMDEC. Le deuxième chapitre a détaillé notre méthodologie, fondée sur une approche qualitative combinant entretiens semi-directifs avec les acteurs clés de BEYN (chef de projet, Product Owner, responsable qualité) et une analyse rigoureuse des données via NVivo et la matrice AMDEC. Enfin, le troisième chapitre a présenté nos résultats, mettant en lumière six catégories de risques (techniques, sécurité/conformité, organisationnels, financiers, délais, externes) et proposant des plans d'action ciblés pour les atténuer.

Les entretiens menés avec les équipes de BEYN ont révélé des défis majeurs, tels que les risques de migration des données, les vulnérabilités de sécurité, ou les retards de développement. L'application de l'AMDEC a permis de hiérarchiser ces risques ( $320 \leq C \leq 400$  nécessitant une intervention immédiate) et de formaliser des réponses adaptées : tests pilotes renforcés, hébergement redondant, authentification multi-facteurs, ou revues régulières des plannings. Malgré les obstacles—comme le temps limité de l'étude, la taille restreinte de l'échantillon (3 employés), ou la complexité des régulations bancaires—, notre recherche démontre que l'AMDEC est un outil puissant pour anticiper et contrôler les risques dans les projets IT, en alignant rigueur méthodologique et flexibilité opérationnelle.

Comme les études que j'ai examinées, ma recherche avait des limites. L'accent mis sur une seule entreprise de fintech signifie que les résultats peuvent ne pas être universellement applicables, ce qui fait écho à la mise en garde de concernant les biais spécifiques au secteur. De futures études pourraient étendre ce travail à des comparaisons interprofessionnelles.

En outre, bien que la méthodologie AMDEC ait été efficace, sa dépendance à l'égard de la notation par des experts introduit de la subjectivité - un défi relevé à la fois dans notre résultat

et dans la critique des matrices de risque formulée par ( Le Coze, et al., 2020). L'intégration d'outils automatisés de détection des risques pourrait renforcer les analyses futures.

Cette recherche se concentre sur un seul cas (BEYN), limitant la généralisation des conclusions. Le contexte algérien, avec ses spécificités réglementaires et technologiques, influence également les résultats.

Malgré ces limites, notre étude offre une contribution pratique aux professionnels du secteur bancaire digital, en prouvant que l'AMDEC—combinée à une culture proactive de gestion des risques—peut renforcer la résilience des projets IT. Les recommandations formulées (formation des équipes, tests itératifs, plans de contingence) fournissent un cadre actionnable pour BEYN et des organisations similaires. À l'ère de la transformation numérique, où les risques évoluent constamment, cette recherche souligne l'urgence d'adopter des méthodologies adaptatives, ancrées à la fois dans la théorie et les réalités opérationnelles.

# **LISTE BIBLIOGRAPHIQUE**

- A Guide to the Project Management Body of Knowledge. (2013). *A Guide to the Project Management Body of Knowledge* (éd. Edition, (PMBOK® Guide) – Fifth). Project Management institute.
- A, W. L. (2003). Agile software development : it's about feedback and change. pp. pp. 39-43.
- Abrahamsson P, S. O. (2002). Agile Software Development Methods Review and Analysis.
- Achibane, A., & Allam, I. (2019, septembre). La gestion des risques bancaires entre l'approche prudentielle et l'approche opérationnelle : cas des Banques Marocaines. *Revue du Contrôle de la Comptabilité et de l'Audit, Volume 4*, 166-195.
- AFNOR. (2003). Gestion des risques projet IT .
- AFNOR. (2010). Management du risque- Principes et lignes directrices. NF ISO 31000.
- AFNOR, N. ( X50-105 Août). *A. F. N. O. R. (2009)*. 1991.
- ALAOUI, M., & DHIBA, Y. (2022). Le management des risques : Cadre théorique . *International Journal of Accounting, Finance, Auditing, Management and Economics* .
- Amansou, S. (2019). *Gestion des risques : fondements théoriques et analyse critique*. Récupéré sur <https://id.erudit.org/iderudit/1068509ar>.
- AMEDZRO St-HILAIRE, W. (2014). Operational risk control & Project effectiveness in Strategic Project management. *Gestion 2000*, 17-47.
- Arvil, B. S., Robert , D. A., & Palmer , J. O. (s.d.). *Educational Research and Appraisal*.
- Atkinson, R. (1999). Effective Organisations. Dans *Re-framing the Thinking for Information Systems Projects Success* (pp. 13-16). cassell, London.
- Baheux, T. (s.d.). *13 types de risques à connaître en gestion de projet*. Récupéré sur <https://www.reussirsesprojets.com>.
- Benoit, A. A., Sylvie , D., Patry, M., & Rivard, S. ( 1998, juin ). Managing the Risk of IT. *Le CIRANO* .
- Bouyssou, J. (1997). *Théorie Générale du Risque*. (É. Economica, Éd.) paris.
- Businessmap. (s.d.). *businessmap*. Récupéré sur <https://businessmap.io/lean-management/implementing-lean-principles>.

- C, B. K. (2004). *Extreme Programming Explained: Embrace Change*.
- Claire Choisy, C. S. (2020). *Analyse de risque d'une ville flottante*. France .
- Claudiu, G. (2007). *PROJECT RISK MANAGEMENT PHASES*.
- Claude., G. (2019, décembre 5). *scribbr*. Consulté le 05 05, 2025, sur <https://www.scribbr.fr/methodologie/etude-quantitative/>.
- Da-Silvaa, L. R., & António , J. (2014). The project risk management process, a preliminary study. *Procedia Technology*, 946.
- De Santis, M. (2020). *La cartographie des processus, outil de management au service de*.
- DIGITAL TPE*. (2023). Consulté le mai 01, 2025, sur <https://digital-tpe-grandest.com/lintelligence-artificielle-dans-la-gestion-des-risques-prevoir-pour-mieux-agir/>.
- Dr. Menaouer, B. (s.d.). *Chapitre 6 Gestion des risques projet IT*. Récupéré sur <https://elearning.enp-oran.dz>.
- El Allame, M. (s.d.). *Blog gestion de projet*. Consulté le 05 07, 2025, sur <https://blog-gestion-de-projet.com/matrice-gestion-des-risques/#t-1683651946850>.
- El Allame, M. (s.d.). *Blog Gestion de Projet*. Consulté le mai 01, 2025, sur <https://blog-gestion-de-projet.com/diagramme-dishikawa/>.
- EMS (Éd.). (2013). Quelques recherches et publications sur la conduite du changement : Quelques thèses récentes sur le risque. *Question(s) de management*, 84-90.
- Ernoul, R. (2010). *Le grand livre de la qualité*. (A. Éditions, Éd.) Paris.
- Familoni, B. T., & Shoetan, P. O. (2024). Cybersecurity in the financial sector: a comparative analysis of the USA and Nigeria. *Computer Science & IT Research Journal*, 850-877.
- FATOUH, K. (2023). *Approche théorique de la gestion des risques.*, (p. 157). Maroc .
- Germain, S. (2025). *IQar*. Récupéré sur <https://www.iqar.fr/blog/portefeuille-gestion-projet/gestion-projet-hybride-agile-waterfall>.
- GIARD, V. (1999). Dans *Gestion de Projets*. Paris: Economica.

- Gidel , T., & Zonghero, W. (2006). Management de projet : Tome 1, Introduction et fondamentaux.
- Gourc, D., & Bougaret, S. (1999). *LE MANAGEMENT DES RISQUES APPLIQUE AU MANAGEMENT*. Récupéré sur HAL open science.
- Gourc, D., & Bougaret, S. (1999). LE MANAGEMENT DES RISQUES APPLIQUE AU MANAGEMENT DES PROJETS ET DE PORTEFEUILLE DE PROJETS EN RECHERCHE ET DEVELOPPEMENT. Paris. Récupéré sur HAL open science.
- GOURINE, R. (2013). ENJEUX ET PERFORMANCE SOCIO ÉCONOMIQUE D' ACTIONS PROACTIVES ET ENJEUX ET PERFORMANCE SOCIO ÉCONOMIQUE D' ACTIONS PROACTIVES ET SOLIDARITÉ.
- Guide IENA. (2017). cartographie des processus et cartographie des risques : comment les mettre en cohérence ?
- ICH. (2005). guideline Q9 on quality risk management. Dans I. C. Use.
- IFACI. (2013). La cartographie des risques. Dans *Groupe Professionnel Assurance* (p. p46). Paris: Institut français de l'audit et du contrôle interne.
- institute, p. m. (2013). *A guide to the project management Body Of knowledge (PMBOK Guide)- Fifth Edition* .
- Institute, P. M. (2017). *Guide du corpus des connaissances en management de projet* (éd. sixième édition ).
- Isaac, S., & Michael , W. (1997). *Handbook in research and evaluation: A collection of principles, methods, and strategies useful in the planning, design, and evaluation of studies in education and the behavioral sciences*. San Diego: Educational and Industrial Testing Services.
- Ivascu, L., & Cioca, L.-I. (2014). Opportunity Risk: Integrated Approach to Risk Management for Creating Enterprise Opportunities.
- Khalil, C. (2011). Les méthodes "agiles" de management de projets informatiques: une analyse "par la pratique". paris .
- KHELIFA , M., & DERRADJI, A. (2016, août). LES RISQUES DES BANQUES ELECTRONIQUES. *Dourassat Iqtisadiya (Études Économiques)*, 402-407.
- Laboratory Risk Assessment Tool. (2021).

- Larson, E. W., & Gray, C. F. (2013). *Project Management : The Managerial Process with MS Project* (éd. 6 édition ). McGraw-Hill.
- Le Coze, J.-C., Boutillon, M., Macron, T., Vallée, A., Masse, F., Plot, E., & Mazri, C. (2020). Transitions et analyses de risques: défis et perspectives. *22e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement (Lambda Mu 22)*. Le Havre, France.
- Manotas Niño, V. P. (2017). Amélioration de la maîtrise des risques dans les projets par l'utilisation des mécanismes de retour d'expérience.
- Manotas Niño, V. P. (2017). Amélioration de la maîtrise des risques dans les projets par l'utilisation des mécanismes de retour d'expérience.
- Marker, A. ( 2021, mars 24). *Smartsheet*. Récupéré sur <https://fr.smartsheet.com/content/entreprise-risk-management-framework-model>.
- Mercier-Laurent, E. (2016, avril). Connaissances et maitrise de risques OUTILS ET BONNES PRATIQUES. Dans *Connaissances et maitrise de risques*.
- Musawir, A. u., Abd-Karim, S. B., & Mohd-Danuri, M. S. (s.d.). Project governance and its role in enabling organizational strategy implementation.
- Normalisation, A. F. (1986). Fascicule de documentation X60-510. Dans AFNOR, *Techniques d'analyse de la fiabilité des systèmes : procédures d'analyse des modes de défaillance et de leurs effets (AMDE)*.
- Patricia, V., & Niño, M. (2017). Amélioration de la maîtrise des risques dans les projets par l'utilisation des mécanismes de retour d'expérience. p. 16.
- Pierandrei, L. (2019). Risk Management. (2e éd.).
- PMI. (2004). A guide to the project management body of knowledge (PMBOK). Newton Square, PA, USA: Project Management Institute.
- PMI. (2014). Project Management Institute, 5 édition. Dans *Guide du corpus des connaissances en management de proje*.
- PMI. (3013). Project Management Institute. Dans *A Guide to the Project Management Body of Knowledge : PMBOK Guide* (éd. 5th edition ). Newtown Square, Pennsylvania.

- Pommeret, B. (2017, 1 déc). *Fiche 06 : Le diagramme de Pareto*. Récupéré sur <https://www.e-marketing.fr/Thematique/academie-1078/fiche-outils-10154/Le-diagramme-de-Pareto-324755.htm>.
- Project Management Institute. (2000). Project Management Institute. Dans *A guide to the project management body of knowledge (PMBOK)*.
- Project Management Institute (PMI). (2017). *A guide to the project management body of knowledge (PMBOK® guide) (6th ed)*. Newton Square, PA: Project Management Institute.
- projet, c. d. (2024, octobre 08). *chef-de-projet.fr*. Récupéré sur <https://chef-de-projet.fr/methode-waterfall/>.
- RAÏS , H. (2012). *GesTion des risques : mesures eT sTrATéGies : AnAlyse empirique DE LA GESTION DES RISQUES DANS LES ENTREPRISES NON FINANCIÈRES FRANÇAISES*.
- Rakoto, H. (2004). *Intégration du Retour d'Expérience dans les processus industriels Application à Alstom Transport*.
- Redsen. (2021, mai 31). Consulté le mai 01, 2025, sur <https://www.redsen.com/project-management/risques-du-management-visuel/>.
- Rodrigues-da-Silva, L. H., & Crispim, J. A. (2014). The project risk management process, a preliminary study. *International Conference on Health and Social Care Information Systems and Technologies* . Braga.
- Roger , A., Crawford, L., & Ward, S. (2006). Fundamental uncertainties in projects and the scope of project management. Dans *International journal of project management* .
- S. Alessandria, A. C. (2018, mai). Probabilistic risk analysis of process plants under seismic loading based on Monte Carlo simulations.
- Scandizzo, S. (2005). Risk mapping and key risk indicators in operational risk management.
- Secureframe. (2024, JULY 11). Récupéré sur <https://secureframe.com/fr-fr/blog/nist-rmf>.
- shizen. (2023, Novembre 7). *shizen* . Récupéré sur <https://shizen.io/six-sigma-comprendre-lean-six-sigma/>.
- Stanisław , G. (2016). *National public projects implementation systems*.

- Suvvari, S. K. (2020). Agile Risk Management: Strategies And Techniques For Mitigating Project Risks.
- Takeushi, H., & Nonaka, I. (1986). The new product development game. *Harvard Business Review*, 137-146.
- Tanzeem, A., Ravi, C. S., Subrahmanyasarma, C., Yellepeddi, S. M., & Pamidi Venkata, A. (2018). Hybrid Project Management: Combining Agile and Traditional.
- Thietart, R. A. (2017). *Méthodes de recherche en management*. (Dunod, Éd.)
- Wendy, C., & Kohn, L. (2014). Les méthodes de recherches qualitatives dans la recherche en soins de santé : Apports et croyances. *Reflets et perspectives de la vie économique*.
- ZARDET, V., & SAVALL, H. (1996). La dimension cognitive de la recherche-intervention : la production de connaissances par interactivité cognitive. *Revue Internationale de Systémique*, Volume 10, 175-189.

# **ANNEXES**

**ANNEXE A :**  
**TABLEAU D'OBSERVATION**

Catégorie d'observation	Critère d'évaluation
<b>Identification des risques</b>	<p>4 types de risque dans un projet de développement :</p> <ol style="list-style-type: none"> <li>1) Développement : - Identification adaptée selon la méthodologie (Agile/Waterfall/Hybride) En Agile : identification continue lors des cérémonies. En Waterfall : identification exhaustive en phase initiale.</li> <li>2) Architecture : Revue d'architecture. Tests de charge préventifs. Évaluation de la scalabilité. Compatibilité des technologies.</li> <li>3) Sécurité : Évaluation des failles potentielles. Tests d'intrusion. Conformité aux standards. Protection des données.</li> <li>4) Fonctionnelle : Clarté des exigences. Ambiguïtés dans les spécifications. Changements de périmètre. Attentes client.</li> </ol>
<b>L'évaluation des risques</b>	<p>Formalisation de l'évaluation</p> <p>Critères de priorisation</p> <p>Implication des parties prenantes</p> <p>Utilisation de méthodes classiques. Matrice de criticité probabilité/impact (échelle 1-5)</p> <p>Réévaluation périodique.</p> <p>Seuils d'intervention</p> <p>Utilisation de registres de risques</p> <p>Documentation adaptée à la méthodologie utilisée</p> <p>Communication transparente avec les clients bancaires</p>
<b>Mesures de prévention et de protection</b>	<p>Plans de mitigation adaptés à chaque projet</p> <p>Approche proactive en Waterfall</p> <p>Actions définies selon priorité dans la matrice de criticité</p> <p>Vigilance continue à travers des revues régulières</p> <p>Signalement des obstacles potentiels lors des Daily standups en Agile</p> <p>Plans de contingence établis avant démarrage du développement</p> <p>Ajustement stratégique en fonction des problèmes émergents</p>
<b>Personnel et formation</b>	<p>Formation continue</p> <p>Certification du personnel</p>

	<p>Partage de connaissances</p> <p>Sensibilisation aux risques</p> <p>Communication ouverte</p> <p>Valorisation de la prévention</p> <p>Retours d'expérience</p>
<b>Réponses aux Risques</b>	<p>Stratégie : Évitement, transfert, atténuation, acceptation</p> <p>Stratégies d'atténuation définies pour les risques identifiés</p> <p>Adaptabilité méthodologique selon nature du projet</p> <p>Approche dynamique et itérative en Agile</p> <p>Détection rapide des problèmes émergents Ajustement stratégique en conséquence</p>
<b>Communication et sensibilisation</b>	<p>Communication lors des cérémonies en Agile</p> <p>Revue périodiques en Waterfall</p> <p>Signalement des obstacles lors des Daily standups</p> <p>Communication transparente avec clients bancaires sur risques identifiés</p> <p>Revue planifiée aux jalons clés avec les clients</p> <p>Registres de risques documentés</p> <p>Plans de mitigation formalisés</p>
<b>Suivi et amélioration</b>	<p>Intégration des enseignements tirés des expériences passées</p> <p>Adaptation des méthodes selon les projets similaires antérieurs</p> <p>Ouverture à l'intégration future d'innovations comme l'IA</p> <p>Révision des processus</p> <p>Mise à jour des méthodes</p> <p>Formation et sensibilisation</p> <p>Benchmarking</p> <p>Analyse post-projet</p> <p>Documentation des leçons apprises</p> <p>Partage des bonnes pratiques</p> <p>Indicateurs de performance (KPI)</p> <p>Tableaux de bord</p> <p>Outils de suivi</p>

**ANNEXE B :**  
**TABLEAU DES VERBATIMS**

Thème	Réponses des interviewé	
Gestion de projet	<p>L'approche de gestion des risques varie en fonction de la méthodologie employée. Dans la méthode Waterfall, nous mettons en place un registre des risques dès le début, avec des examens prévus à des jalons cruciaux. Dans le cadre Agile, nous incorporons cet aspect lors des cérémonies périodiques telles que les planifications de sprint et les rétrospectives, favorisant une détection et un ajustement constant. Dans notre stratégie hybride, nous associons une analyse préliminaire détaillée à des révisions régulières tout au long du processus de développement. Quoi qu'il en soit, nous nous basons sur une matrice de criticité pour hiérarchiser nos actions et assurons une communication claire avec nos clients du secteur bancaire concernant les risques détectés. M.P</p>	
Managem ent des risques	Identificatio n	<ul style="list-style-type: none"> <li>• Dès l'étape d'analyse des spécifications j'identifie les fonctions critiques comme le traitement des transactions, la gestion des erreurs ou la conformité réglementaire. Le paiement étant une fonction assez sensible j'anticipe les scénarios négatifs par exemple que se passerait-il s'il y a une erreur lors de la transaction ou si l'application est assez sécurisée pour le client dans le cas d'un vol ou autre.ASQ</li> <li>• Pour identifier les risques spécifiques aux applications de paiement, nous combinons trois approches complémentaires : une analyse des réglementations bancaires et retours d'expérience du secteur, des ateliers avec experts métier et sécurité pour cibler les vulnérabilités liées aux flux financiers et des tests d'intrusion. MP</li> </ul>
	Évaluation et classificatio n des risques	<ul style="list-style-type: none"> <li>• Nous utilisons une matrice de criticité basée sur deux axes : l'impact (financier, réputationnel, réglementaire, utilisateur) et la probabilité d'occurrence.</li> </ul> <p>Un bug mineur sera par exemple classé comme faible (impact limité, occurrence faible), tandis qu'un risque de fraude ou une faille de sécurité sera automatiquement classé critique, en raison de son impact potentiel sur la confiance des utilisateurs et la conformité légale.</p>

	<p>Chaque risque critique fait l'objet d'un suivi renforcé avec des plans de contingence définis et testés.PO</p> <ul style="list-style-type: none"> <li>• Oui, nous utilisons des outils d'automatisation des tests, notamment pour les tests de régression et de non-régression. Leur mise en place a significativement réduit le taux d'erreurs et nous a permis de gagner un temps considérable dans les cycles de validation. MP</li> </ul>
Amélioration	<ul style="list-style-type: none"> <li>• Non, nous n'avons pas encore implémenté d'approches basées sur l'IA. Cependant, nous restons attentifs aux évolutions.MP</li> <li>• Pour pouvoir capitaliser, il est important de répertorier et de garder une traçabilité des risques rencontrés sur les différents projets c'est cela qui permet de prendre des décisions quant aux améliorations à apporter à la méthodologie et process ASQ</li> <li>• Nous analysons chaque incident via des retours d'expérience formalisés pour identifier les causes racines, ajuster nos processus, et mettre en place des actions préventives afin d'éviter leur récurrence.MP</li> <li>• Nous évaluons l'efficacité de nos nouvelles approches en comparant des indicateurs clés avant et après leur mise en place, notamment le temps de détection des anomalies, la réactivité des équipes et la stabilité des livrables.</li> </ul> <p>Par rapport aux méthodes traditionnelles, les approches récentes (comme l'automatisation des tests ou le travail itératif Agile) nous permettent d'identifier les risques plus tôt, de réduire les retours en phase finale et d'améliorer la qualité globale de nos livrables. Ces gains sont mesurables à travers une baisse du taux de bugs critiques en production et une meilleure satisfaction client.PO</p>

**ANNEXE C:**  
**GUIDE D'ENTERTAIN**

**MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC  
RESEARCH**

**NATIONAL HIGHER SCHOOL OF MANAGEMENT**

**ENSM.KOLÉA.U.C**



# Guide d'entretien

Je suis Benyoucef Dhouha, étudiante en Master 2 Entrepreneuriat et Management de Projet à l'École Nationale Supérieure de Management. Dans le cadre de mémoire de recherche portant sur la gestion des risques dans les projets IT bancaires, je mène une étude approfondie sur le projet AGB de BEYN.

Votre expertise dans ce domaine serait extrêmement précieuse pour notre travail. Je souhaiterais vous poser quelques questions sur, mais avant de commencer, je tiens à vous signaler les éléments suivants : Acceptez-vous que cet entretien soit enregistré, sachant que vos réponses seront utilisées uniquement dans un cadre scientifique pour notre de recherche et ne seront partagés avec personne d'autre.

Section 01 :

Axe 01 : Questions générales

- Pourriez-vous vous présenter ?

- Parlez-nous de votre parcours académique et professionnel
- Pourriez-vous décrire votre rôle et vos responsabilités au sein de votre organisation, et nous présenter brièvement cette dernière ?

## Section 02 :

### Axe 01 : gestion de projet

- Quelle est la méthodologie la plus adaptée dans l'entreprise entre (Agile/Waterfall/Hybride) ?
- "Pouvez-vous décrire comment la gestion des risques est intégrée dans votre méthodologie de management de projet (Agile/Waterfall/Hybride) ?"

### Axe 02 : Approches classiques

- Utilisez-vous des frameworks comme ISO 31000 ou COSO ? Dans quels cas ?"
- "Quels outils classiques de gestion des risques (matrice SWOT, analyse AMDEC) utilisez-vous régulièrement ?"
- "Quelle est votre méthodologie pour identifier les risques spécifiques aux applications de paiement ?"
- "Comment classez-vous les risques en termes de criticité (ex : fraudes vs. bugs mineurs) ?"

### Axe 03 : Approches innovantes

- "Avez-vous implémenté des approches innovantes comme l'IA pour la prédiction des risques ou l'automatisation du suivi ?"
- "Quels sont les avantages et limites de ces outils innovants selon vous ?"
- "Comment mesurez-vous l'efficacité de ces méthodes ?"

### Axe 04 : Amélioration continue

- "Comment évaluez-vous l'efficacité de ces nouvelles approches comparées aux méthodes traditionnelles ?"
- "Comment capitalisez-vous sur les incidents passés pour améliorer vos processus ?"

- Utilisez-vous des outils d'automatisation ou d'IA pour les tests ? Si oui, comment ont-ils amélioré votre gestion des risques ?"

**ANNEXE D :**  
**Entretien de MP**

## Guide d'entretien

Je suis Benyoucef Dhouha, étudiante en Master 2 Entrepreneuriat et Management de Projet à l'École Nationale Supérieure de Management. Dans le cadre de notre mémoire de recherche portant sur la gestion des risques dans les projets IT bancaires, je mène une étude approfondie sur le projet AGB de BEYN.

Votre expertise dans ce domaine serait extrêmement précieuse pour notre travail. Je souhaiterais vous poser quelques questions sur, mais avant de commencer, je tiens à vous signaler les éléments suivants : Acceptez-vous que cet entretien soit enregistré, sachant que vos réponses seront utilisées uniquement dans un cadre scientifique pour notre de recherche et ne seront partagés avec personne d'autre.

Type d'entretien : Semi-Directif.

Section 01 :

### Axe 01 : Questions générales

- **Pourriez-vous vous présenter ?**

**Réponse :** je m'appelle Mohamed TOUBALINE, chef de projet senior chez Beyn. J'ai intégré l'entreprise depuis un peu plus de 2 ans et je suis en charge de différents projets.

- **Parlez-nous de votre parcours académique et professionnel**

- **Réponse :** J'ai décroché mon diplôme de master en systèmes informatiques intelligents à l'Université des Sciences et de la Technologie Houari Boumediene. Cette formation m'a doté d'une forte expertise en informatique avancée, en particulier dans les champs de l'intelligence artificielle et des systèmes d'information complexes.

J'ai entamé mon parcours professionnel comme développeur, ce qui m'a permis d'acquérir une expertise sur divers langages de programmation et de saisir en détail

les défis techniques liés aux projets informatiques. Cette expérience s'est révélée bénéfique pour la continuation de mon cheminement professionnel.

Rapidement, j'ai fait la transition vers la gestion des systèmes d'information, un secteur qui correspondait mieux à ma vision et à mes ambitions professionnelles. Ce changement m'a donné l'occasion de développer plusieurs compétences techniques et de gestion, en particulier dans le domaine de la gestion de projet. Cela m'a donc permis d'acquérir une vision globale des enjeux informatiques en entreprise, en intégrant les dimensions techniques, organisationnelles et humaines. Pour conclure, cela fait un peu plus de deux ans que j'occupe le poste de chef de projet senior au sein de l'équipe Beyn. Dans ce poste, je gère divers projets de numérisation des banques, un domaine en constante évolution technologique. Cette opportunité me donne l'occasion d'appliquer toutes mes compétences dans un cadre stimulant, tout en affrontant les défis propres au domaine bancaire.

- **Pourriez-vous décrire votre rôle et vos responsabilités au sein de votre organisation, et nous présenter brièvement cette dernière ?**
- **Réponse :** Je suis chef de projet senior chez Beyn, une fintech algérienne spécialisée dans les solutions bancaires. Mon rôle consiste à gérer des projets de digitalisation pour les banques, principalement au sein de notre BU Consulting qui développe des solutions sur mesure.

Au quotidien, je coordonne les équipes techniques, assure le suivi des délais et budgets, et maintiens la relation client tout au long du projet. Notre entreprise propose deux modèles d'affaires : des solutions SAAS (software as a service) et des développements spécifiques en acquisition. Cette approche nous permet de répondre efficacement aux différents besoins de transformation numérique du secteur bancaire.

Section 02 :

Axe 01 : gestion de projet

- **Quelle est la méthodologie la plus adaptée dans l'entreprise entre (Agile/Waterfall/Hybride) ?**
- **Réponse :** J'utilise les trois méthodologies Agile, Waterfall et Hybride, selon le contexte. Mon choix s'appuie sur une analyse du projet concerné, des attentes du

client bancaire et des enseignements tirés de nos expériences précédentes. Par exemple, certains projets très réglementés bénéficient de l'approche Waterfall, tandis que des développements plus évolutifs s'adaptent mieux à l'Agile. Souvent, une approche Hybride s'avère être le meilleur compromis pour nos projets de digitalisation bancaire.

- **"Pouvez-vous décrire comment la gestion des risques est intégrée dans votre méthodologie de management de projet (Agile/Waterfall/Hybride) ?"**
- **Réponse :** L'approche de gestion des risques varie en fonction de la méthodologie employée. Dans la méthode Waterfall, nous mettons en place un registre des risques dès le début, avec des examens prévus à des jalons cruciaux. Dans le cadre Agile, nous incorporons cet aspect lors des cérémonies périodiques telles que les planifications de sprint et les rétrospectives, favorisant une détection et un ajustement constant. Dans notre stratégie hybride, nous associons une analyse préliminaire détaillée à des révisions régulières tout au long du processus de développement. Quoi qu'il en soit, nous nous basons sur une matrice de criticité pour hiérarchiser nos actions et assurons une communication claire avec nos clients du secteur bancaire concernant les risques détectés.

#### Axe 02 : Approches classiques

- **Utilisez-vous des frameworks comme ISO 31000 ou COSO ? Dans quels cas ?"**
- **Réponse :** Non, nous n'utilisons pas actuellement ces frameworks comme ISO 31000 ou COSO chez Beyn. Notre approche de gestion des risques s'appuie davantage sur des méthodes adaptées à la taille de nos projets et aux spécificités du secteur bancaire algérien.
- **"Quels outils classiques de gestion des risques (matrice SWOT, analyse AMDEC) utilisez-vous régulièrement ?"**

**Réponse :** Nous utilisons principalement les méthodes classiques de gestion des risques chez Beyn. Notre approche s'appuie sur des outils éprouvés comme la matrice d'analyse de risques probabilité/impact.

- **"Quelle est votre méthodologie pour identifier les risques spécifiques aux applications de paiement ?"**

- **Réponse** : Pour identifier les risques spécifiques aux applications de paiement, nous combinons trois approches complémentaires : une analyse des réglementations bancaires et retours d'expérience du secteur, des ateliers avec experts métier et sécurité pour cibler les vulnérabilités liées aux flux financiers et des tests d'intrusion.
- **"Comment classez-vous les risques en termes de criticité (ex : fraudes vs. bugs mineurs) ?"**
- **Réponse** : Nous classons les risques selon une matrice de criticité qui combine deux dimensions essentielles : la probabilité d'occurrence et l'impact potentiel. Pour chaque risque identifié, nous attribuons un score à ces deux paramètres sur une échelle de 1 à 5.

#### Axe 03 : Approches innovantes

- **"Avez-vous implémenté des approches innovantes comme l'IA pour la prédiction des risques ou l'automatisation du suivi ?"**
- **Réponse** : Non, nous n'avons pas encore implémenté d'approches basées sur l'IA. Cependant, nous restons attentifs aux évolutions.
- **"Quels sont les avantages et limites de ces outils innovants selon vous ?"**
- **Réponse** : Les outils basés sur l'IA présentent des avantages certains. Un traitement rapide de grandes quantités de données, détection précoce d'anomalies et identification de corrélations complexes. Leurs limites dans le secteur bancaire sont toutefois significatives, un besoin important de données historiques et les questions de conformité réglementaire à résoudre.
- **"Comment mesurez-vous l'efficacité de ces méthodes ?"**
- **Réponse** : Comme nous n'utilisons pas encore ces méthodes dans notre processus de gestion des risques, notamment dans le contexte réglementé du secteur bancaire, il ne nous est pas possible d'en mesurer leurs efficacités.

#### Axe 04 : Amélioration continue

- **"Comment évaluez-vous l'efficacité de ces nouvelles approches comparées aux méthodes traditionnelles ?"**
- **Réponse** : N'ayant pas encore adopté ces nouvelles approches, il ne nous est pas possible de les comparer objectivement aux méthodes traditionnelles. Toute comparaison serait prématurée sans retour d'expérience concret.

- **"Comment capitalisez-vous sur les incidents passés pour améliorer vos processus ?"**
- **Réponse :** Nous analysons chaque incident via des retours d'expérience formalisés pour identifier les causes racines, ajuster nos processus, et mettre en place des actions préventives afin d'éviter leur récurrence.
- **Utilisez-vous des outils d'automatisation ou d'IA pour les tests ? Si oui, comment ont-ils amélioré votre gestion des risques ?"**
- **Réponse :** Oui, nous utilisons des outils d'automatisation des tests, notamment pour les tests de régression et de non-régression. Leur mise en place a significativement réduit le taux d'erreurs et nous a permis de gagner un temps considérable dans les cycles de validation.

**ANNEXES E :**  
**Tableau AMDEC**

Opération activités	Mode de défaillance	Effets potentiel	Gravité	Causes probables du défaut	Fréquence	Contrôle de détection	Détection	G*F*D	Plan d'actions	Responsable
Opérationnelle 1	Échec de migration des données	La migration des données de l'ancien e-banking pourrait échouer, entraînant une indisponibilité des comptes clients.	25	Incompatibilité entre les formats de données anciens/nouveaux. - Erreurs dans les scripts de migration personnalisés par BEYN. - Interruptions dues à des problèmes de connectivité avec les systèmes legacy d'AGB..	3	Tests pilotes avec des données réelles d'AGB. - Validation des scripts par l'équipe technique d'AGB avant exécution.	3	225	Effectuer plusieurs tests pilotes et prévoir une stratégie de rollback.	Chef de Projet
Opérationnelle 1	Panne des serveurs en production	Une défaillance des serveurs pourrait entraîner une interruption de service.	20	Défaillance du matériel hébergé chez BEYN. - Configuration incorrecte des serveurs dédiés à AGB.	2	Infrastructure redondante avec <b>cluster HA</b> (High Availability).	2	80	Hébergement sur une infrastructure redondante avec des plans de secours.	Responsable IT AGB
Opérationnelle 1	Erreurs humaines lors des tests UAT	Des erreurs dans la validation utilisateur pourraient retarder la mise en production.	15	Manque de familiarité des testeurs d'AGB avec la nouvelle plateforme BEYN. - Cas de tests non alignés sur les spécifications métiers d'AGB.	2	Formation des testeurs d'AGB par BEYN. - Utilisation d'outils de test comme <b>Selenium</b> pour automatiser les scénarios critiques.	1	30	Formation des testeurs et mise en place d'un guide de validation clair.	Équipe Projet AGB
Opérationnelle 1	Manque de formation des employés	Les équipes internes pourraient ne pas maîtriser la nouvelle plateforme.	15	Planning de formation trop serré. - Contenu de formation non adapté aux besoins.	2	Évaluations post-formation pour mesurer l'acquisition des compétences. - Feedback des employés sur la qualité de la formation.	1	30	Sessions de formation intensives avant le déploiement.	Responsable Formation AGB
Opérationnelle 1	Perte de données lors des migrations	Des fichiers clients ou historiques pourraient être perdus.	15	Problèmes techniques : Une défaillance du support de stockage pendant la migration, une corruption des données lors du transfert ou une interruption imprévue (coupure de courant, problème réseau) peuvent causer des pertes irréversibles.  Incompatibilités logicielles : Si	2	Vérification pré-migration : Avant toute migration, un audit des données doit être réalisé pour s'assurer de leur intégrité et de leur complétude. Une sauvegarde complète doit également être effectuée pour permettre une restauration en cas de problème.  Validation post-migration : Après le transfert, une comparaison entre les données source et destination doit être effectuée, en vérifiant	1	30		Responsable IT AGB, Équipe Développement

				le nouveau système ne prend pas en charge certains formats de fichiers ou si des bugs affectent les outils de migration, des données peuvent être endommagées ou perdues.		le nombre de fichiers, leur taille et leur hachage. Des tests de restauration à partir des sauvegardes confirment la réussite de l'opération.				
<b>Sécurité</b>	Attaque par déni de service (DDoS)	Une attaque DDoS pourrait rendre l'application inutilisable, impactant les services bancaires.	25	Exposition des APIs BEYN aux attaques (cible potentielle pour les cybercriminels). - Absence de mitigation cloud (BEYN n'utilise pas de CDN anti-DDoS).	3	Déploiement de <b>Cloudflare</b> ou <b>AWS Shield</b> pour protéger les endpoints. - Tests de résistance avec des outils comme <b>Kali Linux</b> .	2	150	Mise en place de pare-feu et de services anti-DDoS avancés.	Responsable Sécurité AGB
<b>Sécurité</b>	Faible d'authentification	Une vulnérabilité pourrait être exploitée pour usurper l'identité des utilisateurs.	10	Implémentation défectueuse de la MFA par BEYN. - Vulnérabilités dans le protocole OAuth 2.0 utilisé.	2	Pentests des flux d'authentification par un tiers indépendant.  Revue des logs d'accès via <b>SIEM (ex: Splunk)</b> .	2	40	Implémentation de l'authentification multi-facteurs.	Responsable Sécurité AGB, Équipe Développement
<b>Sécurité</b>	Mauvaise gestion des accès	Des droits d'accès mal configurés pourraient exposer des données sensibles.	10	Absence de revue des accès. - Utilisation de comptes partagés.	2	Audits périodiques des droits d'accès. - Mise en place de workflows d'approbation pour les changements d'accès.	2	40	Mise en place d'un contrôle strict des accès et d'audits réguliers.	Responsable Sécurité AGB
<b>Technique</b>	Instabilité des API du Core Banking	Les API utilisées pour récupérer les données bancaires pourraient être instables, impactant les transactions et les soldes affichés.	25	Intégration complexe entre les APIs BEYN et les systèmes core banking d'AGB (ex: Temenos). - Problèmes de latence dus à l'architecture distribuée.	3	Tests de charge avec <b>JMeter</b> simulant les pics transactionnels d'AGB. - Utilisation de <b>Kong API Gateway</b> pour gérer les requêtes.	3	225	Tests de résilience, mise en place de mécanismes de cache pour assurer la continuité.	Équipe Développement
<b>Technique</b>	Bug critique en production	Un défaut majeur dans le code pourrait affecter les transactions.	20	Code non testé sur des cas d'usage spécifiques à AGB (ex : virements massifs). - Environnement	2	Environnement de staging mirroring la prod d'AGB. - Tests <b>A/B testing</b> pour les fonctionnalités critiques.	3	120	Multiplication des tests QA et mise en place d'un environnement de préproduction.	Équipe QA, Responsable IT AGB

				de préproduction non identique à celui d'AGB.						
<b>Intégration Technique</b>	Intégration complexe de l'API Gateway	L'ajout d'un composant API Gateway au cœur de l'architecture introduit de la complexité dans le routage, la sécurité et le monitoring des échanges API.	20	Incompatibilité entre les systèmes. - Erreurs de configuration des règles de routage ou de sécurité.	2	- Tests de charge et de résilience sur la Gateway. - Documentation détaillée des flux et des configurations.	2	80	Réalisation d'un audit d'architecture, documentation claire des flux, et tests de charge sur la Gateway.	Team-Lead / Architecte BEYN
<b>Technique / Fournisseur</b>	API instables ou inadaptées fournies par le client	Les API exposées par les systèmes AGB présentent des anomalies bloquantes ou ne répondent pas aux spécifications du périmètre.	25	- Bugs non résolus dans les API du fournisseur. - Spécifications techniques non conformes aux attentes.	1	- Escalade rapide des anomalies via Jira et COPROJ.	3	75	Signalement structuré via backlog Jira, remontée au COPROJ, et plan de contournement ou de renforcement IT AGB.	Chef de Projet / Équipe IT AGB
<b>Finance</b>	Dépassement du budget	Le projet pourrait nécessiter des ressources supplémentaires non prévues.	20	Estimation initiale trop optimiste. - Changements non prévus dans le périmètre.	3	Suivi budgétaire mensuel avec rapports détaillés. - Revue des écarts et ajustements si nécessaire.	1	60	Suivi budgétaire rigoureux et contrôle des coûts.	Chef de Projet
<b>Finance</b>	Avenants contractuels non budgétés	Des modifications post-signature du contrat pourraient générer des coûts supplémentaires.	10	Changements de scope non anticipés. - Manque de clarté dans les exigences initiales.	2	Processus strict d'approbation des changements. - Documentation détaillée des avenants. - Revue régulière des engagements contractuels.	1	20	Processus strict d'approbation des changements et suivi budgétaire rigoureux.	Comité de Pilotage (COPIL), Comité de Validation des Changements (CVC)
<b>Performance</b>	Problèmes de scalabilité	L'architecture de la solution pourrait ne pas supporter un grand nombre d'utilisateurs simultanés.	20	Architecture non optimisée pour la charge.	2	Tests de charge pour simuler un grand nombre d'utilisateurs.	2	80	Tests de charge avant la mise en production, optimisation des infrastructures.	Team-Lead
<b>Fonctionnel / Périmètre</b>	Remplacement récurrent de fonctionnalités	Le client formule régulièrement des demandes pour remplacer des fonctionnalités validées, ce qui engendre un décalage dans la planification.	15	- Spécifications techniques non conformes aux attentes. - Problèmes de performance ou de scalabilité côté fournisseur.	3	- Surveillance continue des performances via outils comme Prometheus ou New Relic.	1	45	Mise en place d'un processus de contrôle des changements (CVC) avec évaluation d'impact systématique.	Chef de Projet / CVC
<b>conformité</b>	Non-respect des réglementations	Le projet pourrait ne pas être conforme aux exigences réglementaires, entraînant des retards.	15	Mises à jour non appliquées aux modules de conformité.	2	Intégration des règles métiers dans les workflows BEYN.	2	60	Validation continue avec le département de conformité.	Responsable Conformité AGB
<b>Gestion Projet</b>	Retards de développement	Les fonctionnalités clés pourraient	25	Mauvaise estimation des tâches.	4	Suivi rigoureux des plannings avec des outils comme Jira.	3	300	Suivi strict des plannings, augmentation	Chef de Projet

		être livrées en retard, retardant la mise en production.		- Problèmes techniques non anticipés. - Ressources insuffisantes ou mal gérées.		- Points d'avancement réguliers. - Ajustement des ressources si nécessaire.			temporaire des ressources si nécessaire.	
<b>Utilisateurs</b>	Adoption faible par les clients	Les utilisateurs pourraient ne pas adopter la nouvelle plateforme, entraînant un retour sur investissement limité.	20	Manque de communication sur les nouvelles fonctionnalités.	2	Tests utilisateurs (UX) avec des clients d'AGB.	3	120	Campagnes de formation et communication renforcée avant le lancement.	Équipe Marketing AGB
<b>Organisationnel / Métier</b>	Non-maîtrise fonctionnelle côté client	L'absence de connaissance fonctionnelle approfondie du client sur certains modules (ex : pré-domiciliation, comex) retarde les phases de validation.	10	- Manque d'implication des experts métiers durant les phases clés. - Turnover des responsables métiers.	2	- Implication du Product Owner pour valider les spécifications fonctionnelles.	1	20	Organisation de formations ciblées, implication du Product Owner et renforcement des ateliers métiers.	Chef de Projet AGB / PO
<b>Santé</b>	Pandémie impactant le projet	Une pandémie pourrait ralentir le développement et la mise en production.	20	Retards dans les livraisons BEYN dus au télétravail. - Difficultés d'accès aux environnements sécurisés d'AGB.	1	Utilisation de VPN et accès sécurisés pour les équipes BEYN.	3	60	Mise en place du télétravail et gestion des ressources à distance.	Chef de Projet
<b>Climatique</b>	Catastrophe naturelle	Un sinistre naturel pourrait affecter les infrastructures IT.	25	Sinistre endommageant les infrastructures physiques (centres de données, bureaux). - Interruptions prolongées des services.	1	Sauvegardes externalisées et sécurisées.	3	75	Disaste Recovery (DR)	Responsable IT AGB