

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
القلعة

مذكرة مكملة لنيل شهادة الماستر في الإدارة الإستراتيجية ونظام المعلومات

تخصص: الإدارة الاستراتيجية ونظام المعلومات

إعداد خارطة المخاطر التشغيلية الخاصة ببطاقة الدفع البنكية

دراسة حالة في بنك تراست

من إعداد الطالب:

شعلاني إبراهيم

تحت إشراف الدكتورة:

سمية لعجوزي

تحت إشراف الأستاذة الدكتورة:

جميلة تومي

السنة الجامعية: 2024\2025

ملخص

اعتُبرت المخاطر التشغيلية من أبرز التحديات التي واجهت البنوك، نظراً لطبيعتها غير المتوقعة، حيث كانت تتجم عن أخطاء بشرية، أو فشل في الأنظمة والإجراءات، أو حتى عن عوامل خارجية. وقد أدى ضعف التحكم في هذه المخاطر إلى حدوث خسائر مالية، وفقدان ثقة العملاء، وظهور تهديدات سيبرانية، أو مخاطر نظامية (Risque Systémique) أثرت على استمرارية النشاط البنكي.

وفي هذا السياق، سلّطت هذه الدراسة الضوء على الأدوات والمنهجيات التي كان يعتمدها القطاع البنكي لرصد هذه المخاطر والتعامل معها بشكل استباقي، ومن أبرزها: خارطة المخاطر، المؤشرات الرئيسية للمخاطر (KRI)، وخطط العمل التصحيحية. ورَكَزَت الدراسة بشكل خاص على منهجية التقييم الذاتي للمخاطر والرقابة (RCSA)، التي اعتمدت على إشراك الفرق التشغيلية في تحديد المخاطر وتقييم فعاليتها الضوابط، مما أتاح رؤية شاملة وواقعية للمخاطر.

وقد تم تطبيق هذه المنهجية في إطار دراسة حالة ببنك ترست الجزائر، على منتج البطاقة البنكية، بصفتها المنهجية المعتمدة من طرف البنك. ومن خلال تنظيم ورشة عمل لإعداد خارطة المخاطر التشغيلية، تم تحديد وتقييم المخاطر عبر مختلف مراحل المعالجة باستخدام النظام المعلوماتي Risk Nucleus، مع الأخذ بعين الاعتبار فعالية نظام الرقابة الداخلية. وأظهرت النتائج أن أغلب المخاطر المحددة كانت خاضعة للرقابة وتم التحكم فيها بشكل مناسب، مما عكس فعالية المنهجية والإطار المعتمد لإدارة المخاطر داخل المؤسسة.

الكلمات المفتاحية: المخاطر التشغيلية، بطاقات الدفع، خارطة المخاطر (RCSA)، الرقابة الداخلية، Risk Nucleus.

Résumé

Les risques opérationnels ont été considérés comme l'un des principaux défis auxquels les banques étaient confrontées, en raison de leur nature imprévisible. Ils résultaient souvent d'erreurs humaines, de défaillances des systèmes et des procédures, ou même de facteurs externes. Un contrôle insuffisant de ces risques a conduit à des pertes financières, une perte de confiance des clients, l'apparition de menaces cybernétiques, ainsi que des risques systémiques (Risque Systémique) ayant affecté la continuité de l'activité bancaire.

Dans ce contexte, cette étude a mis en lumière les outils et méthodologies adoptés dans le secteur bancaire pour détecter ces risques et y faire face de manière proactive. Parmi les plus importants figuraient : la cartographie des risques, les indicateurs clés de risque (KRI), et les plans d'action correctifs. L'étude s'est particulièrement concentrée sur la méthodologie d'auto-évaluation des risques et des contrôles (RCSA), qui s'est appuyée sur la participation des équipes opérationnelles dans l'identification des risques et l'évaluation de l'efficacité des contrôles, permettant ainsi une vision globale et réaliste des risques.

Cette méthodologie a été appliquée dans le cadre d'une étude de cas au sein de Trust Bank Algérie, portant sur le produit de la carte bancaire, étant donné qu'il s'agissait de la méthodologie adoptée par la banque. Un atelier a été organisé pour élaborer la cartographie des risques opérationnels, au cours duquel les risques ont été identifiés et évalués à travers les différentes étapes de traitement en utilisant le système d'information Risk Nucleus, tout en tenant compte de l'efficacité du système de contrôle interne. Les résultats ont montré que la majorité des risques identifiés étaient sous contrôle et faisaient l'objet d'une gestion appropriée, ce qui reflétait l'efficacité de la méthodologie et du cadre adopté pour la gestion des risques au sein de l'institution.

Mots-clés : Risques opérationnels, cartes de paiement, cartographie des risques (RCSA), contrôle interne, Risk Nucleus.

Abstract

Operational risks were considered among the main challenges faced by banks due to their unpredictable nature. These risks often stemmed from human errors, system and procedural failures, or even external factors. Inadequate control of such risks led to financial losses, a loss of customer trust, the emergence of cyber threats, and systemic risks (Risque Systémique) that affected the continuity of banking operations.

In this context, the study highlighted the tools and methodologies adopted in the banking sector to detect and proactively manage these risks. Among the most notable were: the risk map, key risk indicators (KRI), and corrective action plans. The study placed particular emphasis on the Risk and Control Self-Assessment (RCSA) methodology, which relied on the involvement of operational teams in identifying risks and assessing the effectiveness of controls, thereby providing a comprehensive and realistic view of risks.

This methodology was applied as part of a case study at Trust Bank Algeria, focusing on the bank card product, as it was the methodology adopted by the bank. A workshop was organized to develop the operational risk map, during which risks were identified and assessed across the different processing stages using the Risk Nucleus information system, while taking into account the effectiveness of the internal control system. The results showed that most of the identified risks were under control and appropriately managed, reflecting the effectiveness of the methodology and the risk management framework adopted by the institution.

Keywords: Operational risks, payment cards, risk map (RCSA), internal control, RISK NUCLEUS.

فهرس المحتويات

I.....	ملخص
VI.....	شكر وتقدير
VII.....	الإهداء
VIII.....	قائمة الجداول
IX.....	قائمة الأشكال
X.....	قائمة الاختصارات
1.....	المقدمة العامة
7.....	الفصل الأول: الدراسة السابقة و الإطار المفاهيمي
8.....	<u>المبحث الأول: مراجعة الدراسات السابقة</u>
8.....	المطلب الأول: الدراسات السابقة حول إدارة المخاطر التشغيلية في البنوك
12.....	المطلب الثاني: تحليل محاور التركيز ومقارنة بين الدراسات
15.....	المطلب الثالث: استخلاص محاور التركيز والتوجهات المستقبلية
17.....	<u>المبحث الثاني: الإطار المفاهيمي</u>
17.....	المطلب الأول : المفاهيم الأساسية لإدارة المخاطر التشغيلية
26.....	المطلب الثاني: مصادر وأسباب وأهمية إدارة المخاطرة
31.....	المطلب الثالث: مراحل إدارة المخاطر التشغيلية
35.....	المطلب الرابع: التدقيق والرقابة الداخلية والتنظيم الاحترازي لمنظومة إدارة لمخاطر
54.....	<u>المبحث الثالث: خارطة المخاطر البنكية</u>
54.....	المطلب الأول: عموميات حول خارطة المخاطر البنكية
58.....	المطلب الثاني: خصائصها وتصنيفاتها في القطاع البنكي
62.....	المطلب الثالث: أدوات ومنهجية إعداد الخارطة
72.....	المطلب الرابع: الاستخدامات الرئيسية لخريطة المخاطر في البنوك

المبحث الرابع : بطاقات الدفع البنكية والمخاطر التشغيلية المرتبطة بها 81

المطلب الأول :التعريف والأنواع والمراحل 81

المطلب الثاني: تصنيف وتحليل المخاطر الخاصة ببطاقات الدفع..... 90

المطلب الثالث: المنهجية الفعالة لتطبيق خارطة مخاطر بطاقات الدفع 95

المطلب الرابع : المخاطر التشغيلية الكامنة الخاصة ببطاقات الدفع البنكية 97

الفصل الثاني: الإطار الميداني و المنهجي..... 101

المبحث الأول: مؤسسة الدراسة 102

المطلب الأول: تقديم المؤسسة المستقبلة - بنك ترست الجزائر 103

المطلب الثاني : الهيكل التنظيمي والخصائص التشغيلية لبنك تراست الجزائر 105

المطلب الثالث : الأنشطة والخدمات المصرفية..... 108

المبحث الثاني :المنهجية البحثية..... 112

المطلب الأول : الموقف الأبيستمولوجيا وطريقة البحث 112

المطلب الثاني :النموذج التحليلي..... 118

المطلب الثالث: النموذج التطبيقي 122

الفصل الثالث: تحليل النتائج و المناقشة 116

المبحث الأول : تحليل العمليات وتحديد المخاطر في بطاقة الدفع 125

المبحث الثاني : تقييم وتحديد وتصنيف المخاطر..... 132

المبحث الثالث: مناقشة النتائج و الإقتراحات 142

الخاتمة 144

المراجع و المصادر 150

الملاحق 153

شكر وتقدير

أنتدّم بخالص الشكر وعظيم الامتنان إلى الدكتورتين ال

فاضلتين سمية لعجوزي وجميلة تومي،

وإلى المشرفين على التربص الميداني: العيد بويوسف، الهادي جرابة، ونسرين زراري،

على ما بذلوه من جهد في تأطير هذا العمل، وعلى توجيهاتهم القيّمة، وصبرهم، وملاحظاتهم البناءة

التي كان لها بالغ الأثر في إنجاز هذه المذكرة.

كما أتوجّه بجزيل الشكر إلى أعضاء لجنة المناقشة الكرام، على قبولهم مناقشة هذا العمل، وعلى ما

سيقدّمونه من ملاحظات وتوجيهات تثري هذا البحث وتُسهّم في تطويره.

ولا يفوتني أن أعبر عن امتناني لكل الأساتذة الذين درسوني ورافقوني خلال سنوات التكوين، ولكل من

قدّم لي يد العون، من قريب أو بعيد، في إعداد هذا العمل، سواء بالدعم العلمي أو المعنوي.

أجدّد شكري وامتناني لكل من كان سندًا لي في هذا المسار، وأخصّ بالذكر عائلتي التي لم تبخل عليّ

بدعمها ودعواتها الصادقة.

الإهداء

إلى من كانت لهم اليد الطولى في مسيرتي العلمية والتكوينية،

إلى من غرسوا في نفسي حبّ العلم والاجتهاد،

وخاصة أستاذي جمال بوكردنة والأستاذة سعاد بلعربي،

إلى والديّ الكريمين، تقديراً وامتناناً لما قدّماه من دعمٍ مادي ومعنوي طيلة سنوات دراستي،

إلى روح والدي ساعد بن إبراهيم بن لحرش،

إلى إخوتي وأخواتي الأعزاء، سندي الدائم في الحياة،

إلى صديقي الوفي براهيم علي فوزي، الذي كان نعم الرفيق والمساند،

إلى بلحمري فاطمة الزهراء، التي كانت لي عوناً كبيراً ودعمًا صادقاً خلال سنوات دراستي في القليعة،

إلى أساتذتي الأفاضل الذين لم يبخلوا عليّ بعلمهم وتوجيهاتهم السديدة، عرفاناً برسالتهم النبيلة،

إلى كل من ساهم، من قريب أو بعيد، في إنجاز هذه المذكرة،

أهدي هذا العمل المتواضع عربون شكر وتقدير وامتنان صادق.

قائمة الجداول

الصفحة	العنوان	رقم الجدول
9	الدراسة السابقة المرتبطة بالموضوع على المستوى العالمي	الجدول 1
11	الدراسات السابقة في المؤسسة الجزائري	الجدول 2
56	الأهمية والأهداف من إعداد خارطة المخاطر البنكية	الجدول 3
94	أنواع المخاطر في بطاقة الدفع البنكية	الجدول 4
97	المخاطر التشغيلية المرتبطة بطاقة الدفع البنكية	الجدول 5
105	المؤشرات الرئيسية لبنك تراست	الجدول 6
110	أنواع الحسابات في تراست بنك	الجدول 7
131	مرحلة التوثيق وفهم العمليات لبطاقة الدفع البنكية	الجدول 8
132	المخاطر الخاصة بطاقة الدفع البنكية	الجدول 9
140	نتائج التقييم الذاتي للمخاطر و الرقابة حسب كل عملية فرعية و عملية تشغيلية	الجدول 10
141	تفاصيل عمليتين أساسيتين في المخاطر التشغيلية المرتبطة بطاقة الدفع البنكية	الجدول 11

قائمة الأشكال

رقم الأشكال	العنوان	الصفحة
الشكل 1	يوضح أهم أنواع المخاطر في الأنشطة البنكية و المصرفية	23
الشكل 2	خطوات عملية إدارة المخاطر	34
الشكل 3	أنظمة إدارة المخاطر البنكية في المنظومة البنكية الجزائرية	45
الشكل 4	مستويات الرقابة على المخاطر البنكية	46
الشكل 5	تسيير الخطر والتنظيم الاحترازي	51
الشكل 6	مصنوفة تصنيف وتقييم المخاطر من خلال التكرار وشدة التأثير	69
الشكل 7	يوضح المؤسسات المصرفية المنتمية إلى الشبكة البنكية للنقديات المشتركة.	82
الشكل 8	العناصر الموجودة على الجهة الأمامية والخلفية للبطاقة البنكية	84
الشكل 9	مراحل عمل بطاقة الدفع عن إجراء عملية شراء عبر جهاز الدفع الإلكتروني	88
الشكل 10	يوضح الشكل مراحل عمل البطاقة في الصراف الألي	90
الشكل 11	الهيكل التنظيمي لبنك تراست	108
الشكل 12	منهجية إدارة المخاطر التشغيلية من خلال التقييم الذاتي للمخاطر والضوابط (RCSA)	114
الشكل 13	إعداد ورشات العمل	115
الشكل 14	مضمون ورشات العمل في تطبيق RISK NUCLEUS	116
الشكل 15	مختلف التقارير الألية في تطبيق RISK NUCLEUS	117
الشكل 16	واجهه تقييم المخاطر وأنظمة الرقابة في تطبيق RISK NUCLEUS	119
الشكل 17	مضمون خطط العمل في تطبيق RISK NUCLEUS	123
الشكل 18	نتائج ورشات تقييم المخاطر الخامة و الصافية في تطبيق RISK NUCLEUS	124
الشكل 19	واجهه دمج نتائج ورشات تقييم المخاطر في تطبيق RISK NUCLEUS	125
الشكل 20	تجزئة النشاطات و العمليات التشغيلية	130
الشكل 21	تحديد و تصنيف المخاطر	135
الشكل 22	مصنوفة تقييم المخاطر	136
الشكل 23	نتائج التقييم الذاتي للمخاطر و الرقابة	137
الشكل 24	نتائج التقييم الذاتي للمخاطر و الرقابة حسب كل عملية فرعية و عملية تشغيلية	138

قائمة الاختصارات

الاختصار	المعنى
AI	Artificial Intelligence (الذكاء الاصطناعي)
API	Application Programming Interface (واجهة برمجة التطبيقات)
AML	Anti-Money Laundering (مكافحة غسل الأموال)
BCBS	Basel Committee on Banking Supervision (لجنة بازل للرقابة المصرفية)
CBDC	Central Bank Digital Currency (العملة الرقمية للبنك المركزي)
COSO	Committee of Sponsoring Organizations of the Treadway Commission
DLP	Data Loss Prevention (منع فقدان البيانات)
DORA	Digital Operational Resilience Act (قانون المرونة التشغيلية الرقمية)
EMV	Europay, MasterCard, and Visa (معياري بطاقات الدفع الذكية)
FAIR	Factor Analysis of Information Risk (تحليل عوامل المخاطر المعلوماتية)
GDPR	General Data Protection Regulation (اللائحة العامة لحماية البيانات)
IMF	International Monetary Fund (صندوق النقد الدولي)
ISO	International Organization for Standardization (المنظمة الدولية للمعايير)
KRI	Key Risk Indicator (مؤشر المخاطر الرئيسية)
PCI DSS	Payment Card Industry Data Security Standard
PIN	Personal Identification Number (الرقم السري)
PSD2	Payment Services Directive 2 (توجيه خدمات الدفع الثاني)
PSD3	Payment Services Directive 3 (توجيه خدمات الدفع الثالث)
RCSA	Risk Control Self-Assessment (التقييم الذاتي للمخاطر والرقابة)
RISK NUCLEUS	اسم نظام تقييم المخاطر المستخدم في الدراسة
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TPP	Third Party Provider (مزود طرف ثالث)

المقدمة العامة

تُعد إدارة المخاطر التشغيلية من الركائز الأساسية لضمان استمرارية المؤسسات المصرفية وسلامة عملياتها، حيث تُشكل خارطة المخاطر أداة استراتيجية لتحليل وتقييم المخاطر المحتملة التي قد تُعيق سير الأنشطة المالية، لاسيما في ظل التحول الرقمي المتسارع في القطاع المصرفي والاعتماد المتزايد على أنظمة الدفع الإلكترونية، وخاصة بطاقات الدفع البنكية. هذا التوسع في استخدام الوسائل الرقمية يستوجب تطوير منهجيات فعالة تُمكن من تعزيز أمن المعاملات وضمان سلاسة استخدامها.

وقد أظهرت التقارير الدولية مؤشرات واضحة على النمو المتسارع في حجم المعاملات غير النقدية، حيث يُتوقع، بحسب تقرير World Payments Report 2025 الصادر عن شركة Capgemini، أن يصل عدد هذه المعاملات إلى نحو 1,650 مليار معاملة بحلول عام 2025، بمعدل نمو سنوي مركب يبلغ 15% بين عامي 2023 و2028، مدفوعًا بانتشار التجارة الإلكترونية وتوسع أنظمة الدفع الفوري. غير أن هذا النمو يصاحبه ارتفاع في حجم الخسائر الناتجة عن الاحتيال باستخدام بطاقات الدفع، إذ سجلت، وفقًا لتقرير (The Nilson Report (2024)، خسائر عالمية بلغت 33.83 مليار دولار أمريكي خلال عام 2023، مقارنة بـ 33.45 مليار دولار في عام 2022، بنسبة زيادة قدرها 1.1%.

وفي السياق الإقليمي، تعكس الأرقام المسجلة في الجزائر هذا التوجه العالمي، إذ بلغ عدد بطاقات الدفع البنكية المتداولة أكثر من 19.3 مليون بطاقة حتى مطلع عام 2025، وشهدت عمليات السحب النقدي باستخدام أجهزة الصراف الآلي ارتفاعًا من 16.63 مليون عملية بقيمة 311.93 مليار دينار جزائري في شهر جانفي، إلى 17.36 مليون عملية بقيمة 330.60 مليار دينار جزائري في شهر فيفري من العام نفسه، وفقًا لإحصائيات (GIE Monétique (2025) كما ارتفع عدد أجهزة الصراف الآلي العاملة إلى 4,072 جهازًا بنهاية فيفري 2025 مقارنة بـ 3,942 جهازًا في نهاية 2024، بزيادة قدرها 130

جهازًا، في حين بلغ عدد محطات الدفع الإلكتروني (TPE) 75,559 جهازًا، بزيادة 7,419 جهازًا خلال شهرين فقط. أما عدد معاملات الدفع الإلكتروني عبر هذه المحطات فقد بلغ 1.3 مليون معاملة بقيمة 11.64 مليار دينار جزائري خلال شهري جانفي وفيفري 2025. كما بلغ إجمالي عدد المعاملات الإلكترونية منذ إطلاق خدمة الدفع عبر الإنترنت باستخدام البطاقات البنكية ما يقارب 60,189,868 معاملة حتى نهاية فيفري 2025، ويُسجل اليوم 625 تاجرًا إلكترونيًا نشطًا ضمن نظام الدفع الإلكتروني بالبطاقات البنكية. (GIE Monétique, 2025),

أما على مستوى بعض الدول المجاورة، فقد بلغ عدد البطاقات البنكية في تونس 5.49 مليون بطاقة حتى نهاية ديسمبر 2024، مُسجّلة تراجعًا بنسبة 22.2% مقارنة بالعام السابق، بحسب البنك المركزي التونسي. (2024) في المقابل، شهدت مصر توسعًا في البنية التحتية للدفع الرقمي، حيث بلغ عدد بطاقات الدفع الإلكتروني فيها 66.2 مليون بطاقة بنهاية ديسمبر 2024، بزيادة تُقدَّر بنحو 13 مليون بطاقة مقارنة بعام 2023، كما تجاوز عدد نقاط البيع الإلكترونية 1.091 مليون نقطة في الفترة نفسها، وفقًا لبيانات البنك المركزي المصري. (2024) أما في المملكة العربية السعودية، فقد سجّل تنفيذ أكثر من 2.5 مليار عملية دفع عبر نقاط البيع في عام 2023، بقيمة إجمالية بلغت 1.4 تريليون ريال سعودي، بحسب (Saudi Central Bank (2024),

وعلى الرغم من هذا التوسع الرقمي، إلا أن المؤسسات المالية في الأسواق الناشئة ما زالت تعاني من ضعف البنية التحتية لإدارة المخاطر التشغيلية، إذ أظهرت دراسة أجرتها (Deloitte (2023 أن 60% من هذه المؤسسات تفتقر إلى أنظمة متكاملة لإدارة المخاطر، مما يزيد من احتمالات تكرار الأخطاء البشرية ويُضعف من فعالية الاستجابة للمخاطر.

بناءً على ذلك تتمحور إشكالية البحث حول السؤال الرئيسي التالي:

كيف يمكننا وضع خارطة المخاطر التشغيلية الخاصة ببطاقات الدفع البنكية من أجل تعزيز سلاسة

وأمن العمليات المالية في بنك تراست؟

وللإجابة على هذه الإشكالية قمنا بتقسيمها إلى الأسئلة الفرعية التالية:

- كيف يمكن توظيف خارطة المخاطر لتحسين إدارة المخاطر والحد من التهديدات التي

تواجه بطاقات الدفع البنكية في بنك تراست؟

- ما هي أفضل الممارسات والتجارب الناجحة في مجال تصميم خارطة مخاطر

للمدفوعات البنكية وكيف يمكن لبنك تراست الاستفادة منها؟

- كيف يمكن إعداد وتنفيذ ورشات عمل داخل بنك تراست لرصد وتقييم وتصنيف

المخاطر التشغيلية الخاصة ببطاقات الدفع؟

- كيف يتم تطبيق مصفوفة تقييم المخاطر التشغيلية (Risk Assessment Matrix)

في بنك تراست لتحديد المخاطر الخامة والصادفة الخاصة ببطاقات الدفع؟

بالاعتماد على الإشكالية والإشكاليات الفرعية التي تم طرحها سابقاً، يمكن استخلاص الأهداف الأساسية

لهذا البحث على النحو الآتي:

أهداف البحث:

تهدف هذه الدراسة إلى تحقيق ما يلي:

- إعداد نموذج تطبيقي متكامل لخارطة المخاطر التشغيلية الخاصة ببطاقات الدفع.

- توظيف منهجية RCSA في تقييم فعالية الضوابط والرقابة الداخلية.
- دعم بنك تراست الجزائر في تحسين قدراته على رصد التهديدات التشغيلية والاستجابة لها بشكل استباقي.
- تعزيز التكامل بين التحليل الكمي والنوعي في إدارة المخاطر التشغيلية.
- اقتراح توصيات عملية قائمة على النتائج الميدانية لتطوير استراتيجيات الحوكمة التشغيلية في البنك .

حيث تم صياغة فرضيات التالية من أجل الدراسة :

- من المتوقع أن تُساهم منهجية التقييم الذاتي للمخاطر (RCSA) في تقديم تصور واقعي لطبيعة المخاطر التشغيلية المرتبطة ببطاقات الدفع البنكية داخل بنك تراست الجزائر .
- قد يُظهر استخدام نظام RISK NUCLEUS فاعلية في الكشف عن النقاط الحساسة في دورة معالجة بطاقات الدفع البنكية.
- يرجح أن يكون إعداد خارطة مخاطر تشغيلية مبني على إشراك الفرق الميدانية مدخلاً فعّالاً لتحسين آليات التقييم الداخلي للمخاطر .
- من المحتمل أن تُسهم خارطة المخاطر التشغيلية في تعزيز القدرة الاستباقية للبنك في مواجهة التهديدات السيبرانية والتنظيمية المتعلقة ببطاقات الدفع.
- من المتوقع أن تؤدي ورشات العمل المعتمدة في إطار البحث إلى تحديد ثغرات في الضوابط الداخلية، مما يسمح بتوجيه الجهود نحو تحسينها.

ومن أجل ذلك اعتمدنا على المنهجية التالية:

منهجية البحث:

تم تبني مقارنة نوعية قائمة على الملاحظة المباشرة، تحليل الوثائق الداخلية، مع مسؤولي بنك تراست الجزائر كما تم اعتماد أسلوب ورشات العمل لتفعيل التقييم الذاتي للمخاطر (RCSA) ، مدعوماً باستخدام نظام معلوماتي متخصص (RISK NUCLEUS) وقد استُخدمت مصفوفات تقييم المخاطر، وتحليل درجة التكرار وشدة التأثير، إلى جانب النمذجة المسبقة للأنشطة، من أجل بناء خارطة دقيقة وقابلة للتحديث.

بعد عرض التساؤلات الرئيسية والفرعية، جاء تنظيم هذا البحث في شكل ثلاثة فصول رئيسية، وذلك على النحو التالي:

➤ المحور الأول: الإطار النظري ومراجعة الدراسة السابقة حيث نستعرض فيه المفاهيم

الأساسية المتعلقة بإدارة المخاطر التشغيلية وخارطة المخاطر في القطاع المصرفي، مع التركيز على المخاطر المرتبطة ببطاقات الدفع.

➤ المحور الثاني: يتناول عرض المؤسسة المضيفة والمنهجية البحثية حيث نقدم نبذة

عن بنك ترست الجزائر ونحدد المنهجية النوعية المتبعة في دراستنا بما في ذلك الأدوات التحليلية مثل المقابلات وتحليل الوثائق لدراسة المخاطر التشغيلية.

➤ المحور الثالث: التطبيق العملي لخارطة المخاطر التشغيلية حيث نقوم بتحليل البيانات

التي تم جمعها من البنك وتقديم نموذج مقترح لخارطة المخاطر التشغيلية الخاصة ببطاقات الدفع في بنك ترست الجزائر مع تقديم تحليل شامل للنتائج والتوصيات المقترحة لتحسين إدارة

المخاطر. تهدف هذه الدراسة إلى تقديم نموذج عملي وقابل للتطبيق لمساعدة البنوك وخاصة بنك ترست الجزائر في تعزيز إدارة المخاطر التشغيلية المتعلقة ببطاقات الدفع البنكية وبالتالي تحسين كفاءة العمليات المالية وضمان حمايتها من التهديدات المحتملة.

الفصل الأول: الدراسة السابقة
والإطار المفاهيمي

المبحث الأول: مراجعة الدراسات السابقة

تُعدّ مراجعة الدراسات السابقة خطوة أساسية لفهم الإسهامات النظرية والتطبيقية حول الموضوع، وتساعد في تأطير الإشكالية وتوجيه البحث ضمن سياقه العلمي المناسب.

المطلب الأول: الدراسات السابقة حول إدارة المخاطر التشغيلية في البنوك

1. مقدمة لدراسة السابقة:

يعد استعراض الأدبيات السابقة من الخطوات الأساسية في أي بحث أكاديمي حيث يوفر فهماً شاملاً للإطار النظري والمفاهيم ذات الصلة بموضوع البحث في دراستنا حول إعداد خارطة المخاطر التشغيلية حالة بطاقات الدفع البنكية في بنك ترست الجزائر قمنا بتحليل مجموعة من الدراسات السابقة التي تناولت إدارة المخاطر التشغيلية في البنوك مع التركيز على المخاطر المتعلقة ببطاقات الدفع.

يهدف هذا الفصل إلى تقديم مراجعة منهجية للأبحاث السابقة مع تسليط الضوء على النتائج الرئيسية التي توصلت إليها ومن ثم تقديم تحليل نقدي لهذه الدراسات من حيث محاور التركيز والجوانب التي لم يتم التركيز عليها بشكل كافٍ.

2. الدراسات السابقة:

يعرض الجدول مجموعة من الدراسات التي تناولت موضوعات متعلقة بإدارة مخاطر الدفع، مثل اكتشاف الاحتيال، أمن بطاقات الدفع، وتقييم التهديدات. يهدف الجدول إلى تقديم نظرة شاملة على الجهود البحثية في هذا المجال من خلال توضيح عناوين الدراسات، مؤلفيها، الدول، سنوات النشر، وأهم النتائج التي توصلت إليها

الجدول رقم 1: الدراسات السابقة المرتبطة بالموضوع على المستوى العالمي

عنوان الدراسة	المؤلفون	السنة	الدولة	أهم النتائج
كشف الاحتيال في أنظمة الدفع	Kumar & Singh	2020	الهند	التطورات التكنولوجية حسّنت من كشف الاحتيال، لكن المجرمين يطورون أساليب جديدة. الحاجة إلى استراتيجيات ديناميكية لمكافحة الاحتيال
المخاطر الأمنية في معاملات بطاقات الدفع	Zhang & Wang	2019	الصين	خروقات الأمان تؤثر على ثقة المستهلكين. أنظمة التشفير والمصادقة متعددة العوامل تقلل من المخاطر، لكنها قد تؤثر على سهولة الاستخدام
أمان بطاقات الدفع: التحديات والحلول	Mishra & Gupta	2022	الهند	التعلم الآلي وتحليل البيانات الضخمة أدوات أساسية لكشف الاحتيال. الحاجة إلى توازن بين الأطر التنظيمية وتكاليف التنفيذ
إدارة المخاطر في أنظمة الدفع	Arora & Rahman	2018	الهند	الامتثال للمعايير الأمنية الدولية يقلل من مخاطر الاحتيال. الحاجة إلى استراتيجيات رقابية مرنة تتكيف مع التهديدات المتغيرة.
دور الأطر التنظيمية في الحد من مخاطر بطاقات الدفع	Nguyen & Tran	2019	فيتنام	الامتثال للوائح المالية يعزز ثقة المستخدمين، لكن تباين القوانين بين الدول يعقد عمليات الامتثال.
إدارة المخاطر في البنوك	Bessis	2015	فرنسا	الإدارة الفعالة للمخاطر التشغيلية تتطلب تغييراً ثقافياً داخل البنوك. الحوكمة القوية ضرورية للحد من المخاطر التشغيلية.
محددات المخاطر التشغيلية في المؤسسات المالية	Chernobai, Jorion & Yu	2010	الولايات المتحدة	حجم البنك وتعقيد عملياته يؤثران على مستوى المخاطر التشغيلية. التكنولوجيا قد تقلل المخاطر التشغيلية لكنها تزيد من التعرض للأمن السيبراني.
إدارة المخاطر التشغيلية في البنوك: مراجعة أدبية	Agarwal & Dhar	2014	الهند	التكنولوجيا الحديثة حسّنت إدارة المخاطر التشغيلية لكنها أدخلت تهديدات جديدة مثل الهجمات الإلكترونية.

تابع للجدول أعلاه 9.

إرشادات تنظيمية لإدارة المخاطر التشغيلية في البنوك	Basel Committee	2011	سويسرا	يجب على البنوك تطوير عمليات صارمة لجمع البيانات حول المخاطر التشغيلية وتحليلها بطرق منهجية.
إدارة المخاطر التشغيلية في البنوك الإفريقية	Akinwumi & Ojo	2018	نيجيريا	تحتاج البنوك الإفريقية إلى تكامل أفضل لاستراتيجيات إدارة المخاطر بسبب القيود التنظيمية والبنية التحتية المحدودة.
تأثير أنظمة الدفع على المخاطر التشغيلية في البنوك الإفريقية	Osei & Agyemang	2020	إفريقيا	نظم الدفع الإلكتروني تقلل بعض المخاطر التشغيلية لكنها تخلق تهديدات جديدة مثل الهجمات السيبرانية.

المصدر: من إعداد الطالب

يوضح الجدول رقم (1) تنوع الدراسات السابقة من حيث الدول والسياقات التي تناولت موضوع المخاطر التشغيلية، حيث ركزت بعض الدراسات على كشف الاحتيال وأمان البيانات بينما تناولت أخرى دور التكنولوجيا الحديثة والذكاء الاصطناعي في مواجهة تلك المخاطر مما يعكس الأهمية المتزايدة لهذا المجال في البيئات المالية المختلفة.

وفيما يلي، سيتم عرض جدول رقم (2) الذي يتناول الدراسات المرتبطة بالمستوى المحلي، لتسليط

الضوء على الجهود المبذولة داخل السياق الوطني في مجال إدارة المخاطر التشغيلية

الجدول رقم 2: الدراسات السابقة في المؤسسات الجزائرية

تواجه البنوك الجزائرية تحديات في تنفيذ استراتيجيات فعالة لرسم خرائط المخاطر التشغيلية بسبب قيود تنظيمية وتقنية.	الجزائر	2019	Bouras & Khelifi	إدارة المخاطر في البنوك الجزائرية
تقنيات رسم خرائط المخاطر التشغيلية توفر رؤية واضحة حول التهديدات المحتملة في أنظمة الدفع الجزائرية.	الجزائر	2020	Zarif & Hossain	تقييم المخاطر التشغيلية في أنظمة الدفع الجزائرية
الامتثال للوائح التنظيمية يحسن من ممارسات إدارة المخاطر التشغيلية، ولكن يتطلب تعاونًا وثيقًا بين الجهات التنظيمية والمؤسسات المالية	الجزائر	2022	Mebarki & Benali	دور الأطر التنظيمية في إدارة المخاطر التشغيلية في الجزائر
على الرغم من أن التكنولوجيا تساهم في تقليل المخاطر التشغيلية، إلا أنها قد تزيد من التهديدات السيبرانية التي تواجه أنظمة الدفع.	الجزائر	2020	Akhter & Hossain	تأثير التكنولوجيا على إدارة المخاطر التشغيلية في الجزائر
تحتاج البنوك الجزائرية إلى تعزيز تدابير الأمن السيبراني لحماية أنظمة الدفع وتقليل المخاطر التشغيلية المرتبطة بها	الجزائر	2021	Zouari & Bouzid	الأمن السيبراني والمخاطر التشغيلية في البنوك الجزائرية

المصدر: من إعداد الطالب

يتضح من خلال الجدول أن المؤسسات المالية الجزائرية وعلى رأسها البنوك تعاني من تحديات تنظيمية وتقنية تعيق تطبيق استراتيجيات فعالة لإدارة المخاطر التشغيلية كما تسلط الدراسات الضوء على أهمية التعاون بين السلطات والجهات التنظيمية والمؤسسات المالية إضافة إلى دور التكنولوجيا والأمن السيبراني في تعزيز حماية أنظمة الدفع وتقليل التهديدات المرتبطة بها وخاصة المخاطر النظامية.

المطلب الثاني: تحليل محاور التركيز ومقارنة بين الدراسات

1. تحليل محاور التركيز في الأدبيات السابقة:

في هذا العنوان سوف نحاول فهم محاور التركيز وبعض الزوايا التي لم تُعالج بعمق في الأدبيات السابقة.

كشف الاحتيال في أنظمة الدفع (Kumar & Singh, 2020)

- ركزت الدراسة على التطورات التكنولوجية لكشف الاحتيال لكنها أغفلت تأثير تطبيق هذه التقنيات على تجربة المستخدم وكفاءة العمليات المصرفية.

المخاطر الأمنية في معاملات بطاقات الدفع (Zhang & Wang, 2019)

- تناولت أنظمة التشفير والمصادقة لكنها لم تدرس تأثيرها على سرعة المعاملات وكفاءة العمليات المصرفية اليومية.

أمان بطاقات الدفع: التحديات والحلول (Mishra & Gupta, 2022)

- ناقشت أهمية التعلم الآلي وتحليل البيانات لكنها لم توضح كيفية تطبيق هذه التقنيات في البنوك ذات الموارد المحدودة.

إدارة المخاطر في أنظمة الدفع (Arora & Rahman, 2018)

- أشارت إلى أهمية الامتثال للمعايير الأمنية لكنها لم تقدم حلولاً عملية للبنوك الصغيرة التي تواجه تحديات في تطبيق هذه المعايير.

دور الأطر التنظيمية في الحد من مخاطر بطاقات الدفع (Nguyen & Tran, 2019)

- تناولت الامتثال للوائح لكنه لم تعالج التحديات التي تواجه البنوك في الامتثال للاختلافات التنظيمية بين الدول.

إدارة المخاطر في البنوك (Bessis, 2015)

- ركزت على الحوكمة القوية لكنها لم تقدم استراتيجيات عملية لتحقيق التغيير الثقافي المطلوب داخل البنوك.

محددات المخاطر التشغيلية في المؤسسات المالية (Chernobai, Jorion & Yu,)

(2010)

- ناقشت تأثير تعقيد عمليات البنك على المخاطر التشغيلية لكنها لم تقدم استراتيجيات لتقليل هذه المخاطر دون التأثير على الكفاءة التشغيلية.

إدارة المخاطر التشغيلية في البنوك: مراجعة أدبية (Agarwal & Dhar, 2014)

- أبرزت تأثير التكنولوجيا الحديثة لكنها أغفلت التحديات المرتبطة بتكامل التقنيات الحديثة مع الأنظمة المصرفية التقليدية.

إرشادات تنظيمية لإدارة المخاطر التشغيلية في البنوك (Basel Committee, 2011)

- حددت ضرورة تطوير عمليات صارمة لجمع البيانات لكنها لم تقدم حلولاً لكيفية تطبيقها في بيئات تنظيمية مختلفة.

إدارة المخاطر التشغيلية في البنوك الإفريقية (Akinwumi & Ojo, 2018)

- ناقشت القيود التنظيمية في إفريقيا لكنها لم تقدم حلولاً واضحة لتجاوز هذه التحديات عبر الابتكار المالي.

تأثير أنظمة الدفع على المخاطر التشغيلية في البنوك الإفريقية (Osei &

(Agyemang, 2020)

- أكدت على تأثير أنظمة الدفع الإلكترونية على تقليل المخاطر لكنها لم تعالج الفجوة الرقمية في البنية التحتية المصرفية الإفريقية.

إدارة المخاطر في البنوك الجزائرية (Bouras & Khelifi, 2019)

- ركزت على القيود التنظيمية لكنها لم تقدم استراتيجيات للتعامل مع هذه التحديات في البنوك الجزائرية.

تقييم المخاطر التشغيلية في أنظمة الدفع الجزائرية (Zarif & Hossain, 2020)

- ناقشت أهمية رسم خرائط المخاطر لكنها لم تقدم حلولاً عملية لتنفيذها في القطاع المصرفي الجزائري.

دور الأطر التنظيمية في إدارة المخاطر التشغيلية في الجزائر (Mebarki & Benali,)

(2022)

- أبرزت أهمية الامتثال للوائح لكنها لم تعالج التأثير المحتمل للمتغيرات الاقتصادية على قدرة البنوك على الامتثال.

الأمن السيبراني والمخاطر التشغيلية في البنوك الجزائرية (Zouari & Bouzid, 2021)

– تناولت تهديدات الأمن السيبراني لكنها لم تقدم تحليلاً لكيفية تحقيق التوازن بين الأمان وتكلفة التنفيذ.

2. تحليل محاور التركيز ومقارنة بين الدراسات:

عند مراجعة الأدبيات لوحظ وجود وجهات نظر مختلفة حول آليات تقييم المخاطر التشغيلية في أنظمة الدفع الإلكتروني حيث ركزت بعض الدراسات على النهج الكمي القائم على تحليل البيانات بينما ركزت أخرى على الأساليب النوعية مثل تحليل الخبراء والمراجعة الدورية للضوابط الأمنية وتم تسجيل التباينات التالية:

- بعض الدراسات أكدت على دور التشريعات الصارمة في تحسين أمن المدفوعات، بينما رأت أخرى أن المرونة في القوانين تتيح مزيداً من الابتكار في مجال أنظمة الدفع.
- تمحورت بعض الأبحاث حول دور العوامل البشرية في المخاطر التشغيلية، بينما ركزت أخرى على تأثير التطورات التكنولوجية.

المطلب الثالث: استخلاص محاور التركيز والتوجهات المستقبلية

1. استخلاص محاور التركيز والتوجهات المستقبلية:

من خلال مراجعة الأدبيات، تم تحديد الفجوات البحثية التالية:

- الحاجة إلى تطوير منهجية أكثر دقة لتقييم المخاطر التشغيلية التي تأخذ بعين الاعتبار التحولات الرقمية الحديثة.

- قلة الدراسات التي تربط بين العوامل الاقتصادية والثقافية وتأثيرها على نجاح نظم الدفع الإلكتروني.

- أهمية تركيز الدراسات حول فعالية أدوات الذكاء الاصطناعي في التنبؤ بالمخاطر التشغيلية.

2. الصعوبات البحثية التي واجهتنا

يواجه الباحث خلال إعداد هذه المذكرة العديد من الصعوبات البحثية من بينها ندرة المراجع المحلية حول إدارة المخاطر التشغيلية في البنوك الجزائرية مما يدفعه إلى الاعتماد على دراسات أجنبية قد لا تتناسب تمامًا مع السياق المحلي كما تشكل صعوبة الحصول على البيانات تحديًا رئيسيًا نظرًا لسرية وخصوصية المعلومات المصرفية المرتبطة بالمخاطر التشغيلية مما يحد من إمكانية الوصول إلى بيانات دقيقة وشاملة بالإضافة إلى ذلك قد يواجه الباحث تحديات منهجية في اختيار الأدوات البحثية المناسبة خاصة في ظل الطبيعة النوعية لبعض البيانات

كما أن التوافق مع التشريعات المصرفية يعد عقبة أخرى حيث تفرض القوانين والأنظمة المصرفية قيودًا على تحليل بعض الجوانب المتعلقة بالمخاطر التشغيلية علاوة على ذلك، يمثل تطبيق المفاهيم النظرية على الواقع العملي تحديًا حيث قد يكون من الصعب تحويل النماذج النظرية إلى حلول عملية قابلة للتطبيق داخل بيئة مصرفية جزائرية محددة.

كما أن التطورات السريعة في التكنولوجيا المالية تزيد من تعقيد البحث نظرًا لأن الابتكارات المستمرة في أنظمة الدفع قد تجعل بعض النتائج بحاجة إلى تحديث متكرر.

وأخيرًا، يعد قياس فعالية النماذج المقترحة لخارطة المخاطر التشغيلية أمرًا معقدًا إذ يصعب محاكاة جميع سيناريوهات المخاطر في بيئة البحث مما يؤثر على دقة النتائج وإمكانية تطبيقها عمليًا.

المبحث الثاني: الإطار المفاهيمي

المطلب الأول : المفاهيم الأساسية لإدارة المخاطر التشغيلية

يمثل الإطار المفاهيمي أحد الركائز الأساسية لأي بحث أكاديمي حيث يساهم في بناء قاعدة معرفية متينة تساعد على فهم الموضوع المطروح من خلال تحديد المفاهيم والمصطلحات الأساسية المرتبطة به في سياق هذه الدراسة يكتسب الإطار المفاهيمي أهمية خاصة إذ يتناول موضوع إدارة المخاطر التشغيلية في البنوك مع التركيز على خارطة المخاطر الخاصة ببطاقات الدفع البنكية ويهدف هذا الإطار إلى تقديم تعريف دقيق للمفاهيم المرتبطة بالمخاطر التشغيلية وآليات تقييمها وأهم النماذج والنظريات التي تم تطويرها في هذا المجال.

1. تعريف المخاطر بصفة عامة والمخاطر التشغيلية بصفة خاصة:

تُعتبر المفاهيم المرتبطة بالمخاطر من الركائز الأساسية لفهم التحديات التي تواجه المؤسسات في بيئاتها المختلفة ويشمل ذلك تعريف المخاطر بشكل عام والمخاطر التشغيلية كأحد أنواعها الأكثر تأثيراً والذي يمثل الإطار المنهجي للتعامل مع هذه التهديدات يساعد التمييز بين هذه المفاهيم في بناء رؤية واضحة شاملة لكيفية التعامل مع المخاطر داخل البنك.

1.1. تعريف المخاطر:

وفقاً للتنظيم رقم 08-11 لبنك الجزائر المؤرخ في 28 نوفمبر 2011 المتعلق بالرقابة الداخلية في البنوك والمؤسسات المالية تم في المادة -2 تعريف تسع فئات رئيسية من المخاطر التي يجب على البنوك والمؤسسات المالية مراقبتها وإدارتها ضمن إطار رقابي داخلي فعال وفيما يلي التعريفات القانونية الخاصة بكل خطر:

2.1. مخاطر الائتمان:

وهي المخاطر الناجمة عن احتمال تعثر طرف مقابل أو مجموعة أطراف يُنظر إليها كمستفيد واحد حسب أحكام المادة 2 من التنظيم رقم 09-91 المعدل والمتمم المتعلق بالقواعد الحذرة لتسيير البنوك والمؤسسات المالية.

3.1. مخاطر التركيز:

تتعلق هذه الفئة بمخاطر منح تسهيلات مالية لطرف واحد أو لأطراف مترابطة أو لنشاط اقتصادي معين أو منطقة جغرافية واحدة بما في ذلك المخاطر الناتجة عن الاعتماد المفرط على ضمانات صادرة عن نفس الجهة.

4.1. مخاطر معدل الفائدة الإجمالي:

وهي المخاطر الناجمة عن تقلبات معدلات الفائدة، نتيجة للأنشطة داخل وخارج الميزانية، باستثناء تلك الخاضعة لمخاطر السوق.

5.1. مخاطر التسوية:

تنشأ هذه المخاطر لا سيما في العمليات بالعملات الأجنبية، أثناء الفترة الممتدة بين اللحظة التي تصبح فيها تعليمات الدفع غير قابلة للإلغاء ولحظة الاستلام الفعلي للأموال أو الأدوات المالية المقابلة وتشمل مخاطر عدم وفاء الطرف المقابل ومخاطر عدم تسليم الأدوات المالية.

6.1. مخاطر السوق:

تشمل الخسائر المحتملة الناتجة عن تقلبات أسعار السوق والتي تؤثر على مراكز الميزانية وخارج الميزانية وتشمل:

- المخاطر المتعلقة بالأدوات المرتبطة بمعدلات الفائدة والأسهم ضمن محفظة التداول
- مخاطر أسعار الصرف.

7.1. مخاطر السيولة:

وهي المخاطر المتعلقة بعدم قدرة المؤسسة على الوفاء بالتزاماتها أو تصفية مراكزها المالية ضمن آجال مناسبة وبتكاليف معقولة بسبب ظروف السوق.

8.1. المخاطر القانونية:

وهي المخاطر المرتبطة بإمكانية نشوء نزاعات قانونية نتيجة لثغرات أو نقائص أو أخطاء في العمليات أو العقود أو الالتزامات التي تكون المؤسسة طرفاً فيها.

9.1. مخاطر عدم الامتثال:

تتمثل في التعرض لعقوبات قضائية أو إدارية أو تأديبية أو لخسائر مالية كبيرة أو أضرار تمس السمعة نتيجة لعدم احترام القوانين والتنظيمات السارية أو المعايير المهنية والأخلاقية أو التعليمات الصادرة عن الهيئات التنظيمية.

10.1. الخطر العملي (التشغيلي):

خطر ناتج عن عدم التأقلم أو أخطاء قد تتسبب إلى الإجراءات أو المستخدمين أو الأنظمة الداخلية، أو العوامل الخارجية ويشمل مخاطر الغش الداخلي والخارجي.

أما المعيار الدولي ISO 31000 الذي يستند إلى الدليل 73:2009 المعني بإدارة المخاطر

والمصطلحات ذات الصلة فيُعرّف الخطر على أنه "تأثير عدم اليقين على تحقيق الأهداف"، حيث يمكن أن يكون هذا التأثير إيجابياً أو سلبياً مقارنة بالتوقعات.

انطلاقاً من مختلف التعاريف المقدمة في التنظيم رقم 11-08 لبنك الجزائر، إلى جانب التعريف المعتمد في المعيار الدولي ISO 31000 يمكن القول إن مفهوم الخطر يشير إلى إمكانية وقوع أحداث أو أوضاع غير متوقعة قد تؤثر سلباً أو إيجاباً على تحقيق أهداف المؤسسة وتتنوع طبيعة هذه المخاطر بحسب مصدرها وتأثيرها، فمنها ما هو مالي أو قانوني أو تشغيلي أو استراتيجي، ومنها ما يرتبط بتقلبات السوق أو بالتغيرات التنظيمية أو بالعوامل الداخلية كالأفراد والأنظمة والعمليات. ويؤكد هذا التعدد في مصادر المخاطر وتشابك آثارها ضرورة تبني مقاربات شاملة لإدارة المخاطر، تأخذ في الحسبان البعد الوقائي، وآليات التخفيف، والاستجابة الفعالة لضمان استمرارية النشاط وتحقيق الأهداف بأعلى درجات الفعالية والكفاءة.

وبناءً على ما سبق، يمكن تعريف المخاطر بصفة عامة على النحو التالي: المخاطر هي احتمالية وقوع أحداث غير مؤكدة قد تؤثر على تحقيق أهداف المؤسسة ولها أبعاد مالية، تشغيلية، قانونية، تنظيمية، وتكنولوجية، مما يستدعي إدارة فعّالة واستباقية لها ضمن إطار شامل لإدارة المخاطر.

2. تعريف المخاطر التشغيلية:

تُعد المخاطر التشغيلية من العناصر الجوهرية في إطار إدارة المخاطر البنكية نظراً لتأثيرها المباشر على كفاءة واستقرار العمليات الداخلية وفيما يلي تعريف هذا النوع من المخاطر:

1.2. وفقاً لبازل 2:

"الخسارة الناتجة عن عدم كفاية أو فشل في العمليات الداخلية أو الأفراد أو الأنظمة أو من أحداث خارجية." (BCBS, 2005).

تحديثات بازل 3 (2011) للمخاطر التشغيلية:

تعريف المخاطر التشغيلية في بازل 3:

في إطار بازل 3 (2011) تظل المخاطر التشغيلية تُعرّف كما كانت في بازل 2 ولكن مع إضافة بعض التوجيهات والتعديلات لتحسين إدارة هذه المخاطر بشكل شامل.

وفقاً لبازل 3، تُعرّف المخاطر التشغيلية بأنها:

"الخسارة الناتجة عن عدم كفاية أو فشل في العمليات الداخلية، أو الأفراد، أو الأنظمة، أو من أحداث خارجية وتشمل المخاطر القانونية ويستثنى منها المخاطر الاستراتيجية والمخاطر المتعلقة بالسمعة" (BCBS, 2011).

2.2. وفقاً لتعريف البنك الدولي (World Bank) تُعرف المخاطر التشغيلية (Operational Risk)

(Risk) على النحو التالي:

"هي المخاطر الناتجة عن قصور أو فشل في العمليات الداخلية أو الأشخاص أو الأنظمة، أو من أحداث خارجية ويشمل ذلك المخاطر القانونية، لكنه لا يشمل المخاطر الناشئة عن القرارات الاستراتيجية أو فقدان السمعة." (World Bank, 2023)

3.2. وفقاً لصندوق النقد الدولي (International Monetary Fund - IMF)،

تُعرف المخاطر التشغيلية على النحو التالي:

"المخاطر التشغيلية هي الخسائر المحتملة الناتجة عن عدم كفاية أو فشل في العمليات الداخلية، أو الأشخاص، أو الأنظمة، أو نتيجة أحداث خارجية. وتشمل هذه الفئة من المخاطر كذلك المخاطر القانونية، لكنها لا تشمل المخاطر الناتجة عن القرارات الاستراتيجية أو السمعة." (IMF, 2023)

ويشمل هذا التعريف بحسب صندوق النقد الدولي مجموعة واسعة من المخاطر مثل:

- الأخطاء البشرية،
- الأعطال التكنولوجية،
- الاحتيال الداخلي أو الخارجي،
- الكوارث الطبيعية،
- والهجمات السيبرانية.

انطلاقاً من هذه التعاريف يمكننا أن نلاحظ أن هناك اتفاقاً بين الهيئات الوطنية والدولية على أن المخاطر التشغيلية تنشأ نتيجة لفشل داخلي في العمليات الأنظمة أو الأفراد إلى جانب العوامل الخارجية مثل الأحداث غير المتوقعة أو التغيرات القانونية.

كما تتسم هذه المخاطر بطبيعتها المتعددة الأبعاد إذ تشمل الجوانب التقنية التنظيمية البشرية والقانونية وهو ما يفرض على المؤسسات المالية اعتماد آليات شاملة لإدارتها.

وبناءً على ما سبق يمكننا اقتراح تعريف تركيبي للمخاطر التشغيلية على النحو التالي:

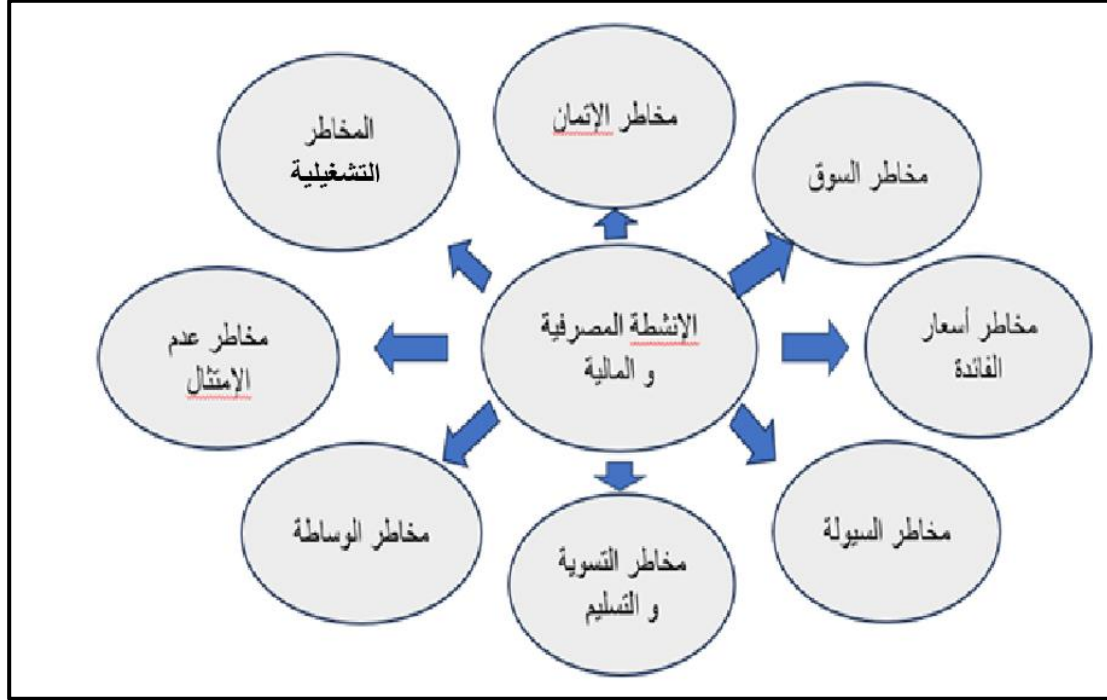
المخاطر التشغيلية هي الخسائر المحتملة التي قد تتعرض لها المؤسسات المالية نتيجة إخفاق أو قصور في العمليات الداخلية أو الأنظمة التقنية أو الموارد البشرية أو نتيجة أحداث خارجية غير متوقعة وتشمل في ذلك المخاطر القانونية والتنظيمية والاحتياطية بما يؤثر على استمرارية العمل.

3. أنواع المخاطر:

يعرض الشكل مجموعة من أنواع المخاطر المرتبطة بالأنشطة المصرفية والمالية، مثل مخاطر الائتمان، مخاطر السوق، مخاطر أسعار الفائدة، ومخاطر السيولة. يهدف الشكل إلى تقديم نظرة شاملة على طبيعة هذه المخاطر من خلال تصنيفها وتوضيح ارتباطها المباشر بالعمليات المصرفية، بما يساعد في

فهم البيئة المعقدة التي تعمل فيها المؤسسات المالية، ويسلط الضوء على أهمية إدارة المخاطر لضمان الاستقرار والكفاءة التشغيلية.

الشكل 1: يوضح أهم أنواع المخاطر في الأنشطة البنكية والمصرفية



المصدر: من إعدادنا باستعانة بالمصادر التالية (Idroj, 2018; BCBS, 2005)

4. تعريف إدارة المخاطر:

تُعد إدارة المخاطر أحد المكونات الأساسية في الحوكمة المؤسسية حيث تهدف إلى تحديد المخاطر المحتملة التي قد تؤثر على تحقيق الأهداف وتحليلها ثم اتخاذ الإجراءات المناسبة للتقليل من آثارها وفيما يلي تعريف إدارة المخاطر:

1.4. تعريف إدارة المخاطر وفق بازل 2 و 3:

تُعرف إدارة المخاطر في السياق المصرفي على أنها "مجموعة العمليات والأساليب التي تهدف إلى تحديد المخاطر وقياسها ومراقبتها والتقليل من آثارها بما يتناسب مع طبيعة نشاط المؤسسة المالية وتعقيد عملياتها. (BCBS, 2005).

4.2. في إطار اتفاقية بازل 2:

ركزت لجنة بازل على أهمية إدماج إدارة المخاطر ضمن الإطار الاستراتيجي للبنوك، مع التركيز على ثلاث فئات رئيسية من المخاطر: مخاطر الائتمان، مخاطر السوق، والمخاطر التشغيلية كما شددت على أهمية أن تمتلك البنوك أنظمة داخلية فعالة لتقدير رأس المال المناسب لمواجهة هذه المخاطر، بما يتجاوز الحد الأدنى التنظيمي (BCBS, 2005)

4.3. أما في اتفاقية بازل 3:

فقد تطورت المفاهيم لتشمل تحسين جودة رأس المال، وضبط مخاطر السيولة، والرافعة المالية، والمخاطر النظامية. هدفت بازل 3 إلى تعزيز قدرة النظام المالي على الصمود أمام الأزمات والصدمات الاقتصادية، عبر أدوات رقابية أكثر شمولاً وصرامة (BCBS, 2011).

في الإطار التنظيمي الجزائري، تُعد إدارة المخاطر من المهام الأساسية التي تلتزم بها البنوك والمؤسسات المالية.

وقد نص القانون رقم 23-09 المؤرخ في 21 جوان 2023، المتعلق بالقانون النقدي والمصرفي، في مواده من 107 إلى 109، على ضرورة: "وضع نظام فعال للرقابة الداخلية، يشمل عمليات تنظيمية وإجراءات تتيح التعرف على المخاطر التي قد تواجه البنك، وقياسها، ومتابعتها، والحد منها، بما يضمن الامتثال للقوانين، ويؤمن سلامة الأصول، ويضمن موثوقية المعلومات المالية وحسن سير العمليات".

انطلاقاً من هذه التعاريف يمكننا أن نلاحظ أن إدارة المخاطر تُعد وظيفة محورية في المؤسسات المالية وتتركز على تحديد التهديدات المحتملة وتحليلها ووضع استراتيجيات للتعامل معها.

كما تؤكد الأدبيات على أهمية دمج الأبعاد التقنية التنظيمية والحوكمة ضمن إطار شمولي يهدف إلى تقليل الخسائر وضمان الامتثال وتعزيز استمرارية العمال.

وتشير التعاريف أيضاً إلى ضرورة التوازن بين الرقابة والنجاعة في مواجهة المخاطر المتغيرة باستمرار.

وبناءً على ذلك يمكن اقتراح تعريف تركيبي لإدارة المخاطر كما يلي: إدارة المخاطر هي عملية منهجية تهدف إلى تحديد وتحليل وتقييم المخاطر المحتملة وتصميم وتنفيذ استراتيجيات رقابية ووقائية مناسبة لضمان حماية موارد المؤسسة وتعزيز استقرارها المالي وضمان استمرارية أنشطتها في بيئة تنظيمية وتشغيلية متغيرة.

5. نظريات تقييم المخاطر التشغيلية:

من خلال الدراسة السابقة تبين أنه توجد ثلاث نظريات يتم الاستناد إليها في تقييم المخاطر التشغيلية وهي:

نظرية الاحتمالات والتحليل الإحصائي: قياس وتقدير المخاطر التشغيلية.

نظرية التحكم في الأنظمة: استخدام الضوابط الداخلية لتقليل المخاطر

نظرية التكلفة والفائدة: موازنة التكاليف المرتبطة بإدارة المخاطر مقابل المنافع المتوقعة.

المطلب الثاني: مصادر وأسباب وأهمية إدارة المخاطرة

1. مصادر المخاطر التشغيلية:

تعد المخاطر التشغيلية من التحديات الرئيسية التي تواجه المؤسسات المالية حيث تنشأ من عدة مصادر تؤثر على استمرارية وكفاءة العمليات ومن أهمها:

1.1. المصادر البشرية: تشمل الأخطاء البشرية الإهمال والاحتيايل الداخلي الذي قد يؤدي إلى خسائر مالية كبيرة (Onyiriuba, 2016).

نقص التدريب وضعف الالتزام بالإجراءات التشغيلية يسهمان في زيادة هذه المخاطر (Loader, 2006).

2.1. المصادر التقنية:

الاعتماد المتزايد على الأنظمة التكنولوجية يزيد من التعرض للمخاطر السيبرانية والاختراقات الأمنية مما يؤثر على استمرارية العمال (Agarwal & Dhar, 2014).

الأعطال التقنية وأخطاء البرمجة قد تعطل العمليات التشغيلية وتؤدي إلى خسائر (Bessis, 2015).

3.1. المصادر التنظيمية والقانونية:

عدم الامتثال للقوانين والتشريعات الوطنية والاتفاقيات الدولية مثل بازل II و III قد يعرض المؤسسات لعقوبات مالية وقانونية مما يؤثر على سمعتها وأدائها المالي (BCBS, 2011).

4.1. المخاطر الناجمة عن الأطراف الثالثة:

تتضمن المخاطر الناتجة عن الاعتماد على مزودي الخدمات الخارجيين مثل فشل الشركاء أو الموردين في تقديم الخدمات المطلوبة بالجودة والوقت المحدد (Bellini, 2016).

5.1. المخاطر البيئية والكوارث الطبيعية:

تشمل الكوارث الطبيعية مثل الزلازل الفيضانات والأعاصير التي قد تؤثر على استمرارية الأعمال وتسبب خسائر مالية (Gregoriou, 2009).

كما أن الأزمات الصحية مثل الجوائح قد تعطل العمليات التشغيلية (Mebarki & Benali, 2022).

6.1. المصادر المرتبطة بالحوكمة وسوء الإدارة:

ضعف أنظمة الحوكمة والرقابة الداخلية يؤدي إلى تفاقم المخاطر التشغيلية نتيجة لسوء أو عدم اتخاذ القرار أو غياب الرقابة الفعالة (Girling, 2013).

2. الأسباب الكامنة وراء المخاطر

وفقاً لما ورد في (Girling, 2013; Loader, 2006; Laycock, 2014)، يمكن تصنيف أسباب المخاطر إلى فئتين رئيسيتين:

– الأسباب الموضوعية: وهي العوامل التي تنشأ بغض النظر عن تدخل الإنسان، مثل العوامل البيئية، الاقتصادية أو التكنولوجية (Laycock, 2014).

– الأسباب الذاتية: وهي العوامل التي تنتج عن تصرفات الإنسان، سواء عن طريق الأخطاء البشرية، الإهمال، الاحتيال أو سوء التسيير (Loader, 2006).

بالإضافة إلى ذلك، يميز (Girling, 2013) بين نوعين من المخاطر عند تقييم تأثيرها على المؤسسات المالية:

– المخاطر الكامنة (المخاطر الخامة):

وهي المخاطر على شكلها الطبيعي والتي لا تخضع لأي وسائل رقابة أو إدارة، حيث تغيب الإجراءات الوقائية، أنشطة الرقابة، أو الأنظمة التكنولوجية التي تحد منها (Laycock, 2014).

– المخاطر المتبقية (المخاطر الصافية):

وهي المخاطر التي تظل قائمة بعد تنفيذ استراتيجيات التحكم، مثل آليات الرقابة الداخلية، التغطية المالية، أو تقنيات توزيع المخاطر (Girling, 2013).

يتضح من خلال هذه التصنيفات أن إدارة المخاطر تتطلب فهماً دقيقاً لطبيعة المخاطر وأسبابها، مما يساعد في تصميم آليات فعالة للتخفيف من تأثيراتها على المؤسسات المالية (Onyiriuba, 2016).

3. أهمية إدارة المخاطر التشغيلية:

إدارة المخاطر التشغيلية تعد أمراً حيوياً لضمان استمرارية ونجاح المنظمات في بيئة أعمال مليئة بالتحديات تساعد في تقليل الخسائر وتحقيق الكفاءة والفعالية، من خلال تحديد وتقييم المخاطر والتعامل معها بشكل استباقي تسهم هذه الإدارة في تعزيز قدرة المنظمة على التكيف مع التغيرات والنمو في بيئة العمل المتقلبة.

1.3. المساعدة في اتخاذ القرار الاستراتيجي:

توفر إدارة المخاطر التشغيلية بيانات وتحليلات دقيقة تساعد في اتخاذ قرارات مستنيرة تعتمد على تقييم المخاطر المحتملة وتحين طرق العمل (Mebarki & Benali, 2022).

2.3. تحقيق ميزة تنافسية في الأسواق المالية:

المؤسسات التي تتبنى نهجًا قويًا في إدارة المخاطر التشغيلية تتمتع بميزة تنافسية لأنها تكون أكثر استعدادًا للتعامل مع الأزمات مقارنة بالمنافسين (Bellini, 2016).

3.3. تحسين أداء العمليات الداخلية:

الإدارة الفعالة للمخاطر التشغيلية تساعد في تقليل الأعطال التقنية والأخطاء البشرية، مما يؤدي إلى تحسين العمليات الداخلية (Onyiriuba, 2016).

4.3. تعزيز سمعة المؤسسة وثقة المستثمرين:

الإدارة الجيدة للمخاطر التشغيلية تعزز الشفافية والحوكمة الرشيدة، مما يؤدي إلى تحسين سمعة المؤسسة وزيادة ثقة المستثمرين (Bessis, 2015).

5.3. زيادة القدرة على مواجهة التغيرات التكنولوجية:

مع تزايد التهديدات الإلكترونية، أصبحت الحاجة لإدارة المخاطر التشغيلية أكثر أهمية لضمان الأمن السيبراني والاستجابة السريعة للأزمات (Agarwal & Dhar, 2014).

6.3. حماية أصول المؤسسات المالية وعملائها:

تقليل المخاطر التشغيلية يساهم في حماية الأصول المالية والمعلومات الحساسة للعملاء مما يعزز الثقة في المؤسسات المالية (Girling, 2013).

7.3. تحسين الامتثال للمعايير التنظيمية:

الامتثال للقوانين والمعايير التنظيمية الوطنية والدولية مثل اتفاقية بازل II و III يساعد في تجنب العقوبات وتعزيز سمعة المؤسسة (BCBS 2011).

4. الأطراف المعنية بإدارة المخاطر المصرفية:

تعدّ إدارة المخاطر عنصراً جوهرياً في الحوكمة الرشيدة للمؤسسات المالية، حيث تتطلب مشاركة فعالة من مختلف الأطراف ذات العلاقة لضمان فعالية السياسات والإجراءات المعتمدة وتتنوع هذه الأطراف بحسب موقعها في النظام المالي ودورها في التأثير على القرارات أو الرقابة، ويمكن تصنيفها على النحو التالي:

- الهيئات التنظيمية والمشرعين الذين يضعون القوانين المصرفية (Collier, 2009).
- المشرفين والمساهمين والمديرين التنفيذيين الذين يراقبون التنفيذ ويضمنون الامتثال (Loader, 2006).
- المشرفون على إدارة المخاطر الذين يتميزون بدور محوري في تصميم وتنفيذ ومتابعة سياسات إدارة المخاطر داخل المؤسسة المالية (Agustina & Rahmatika, 2024).
- المدققين الداخليين والخارجيين الذين يقيمون مدى فاعلية سياسات إدارة المخاطر (Onyiriuba, 2016).
- الجمهور العام، الذي يؤثر ويتأثر بآليات إدارة المخاطر المصرفية (Bellini, 2016).

5. أهداف إدارة المخاطر في البنوك:

- بحسب Cruz (2009) و Gregoriou (2002)، تهدف إدارة المخاطر إلى تحقيق الأهداف التالية:
- تحديد وتحليل المخاطر المحتملة والفرص المرتبطة بها.
- استباق المخاطر واتخاذ التدابير الوقائية بدلاً من التعامل معها بعد وقوعها (Laycock, 2014).
 - حماية الأصول وضمان أمن الودائع، مما يعزز الثقة في النظام المصرفي (Girling, 2013).

- دعم عملية اتخاذ القرار والإدارة الاستراتيجية من خلال تقييم المخاطر بشكل شامل (Collier, 2009).

- تخصيص الموارد بشكل فعال لمواجهة المخاطر الكبرى وتقليل آثارها السلبية (Bellini, 2016).

المطلب الثالث: مراحل إدارة المخاطر التشغيلية

1. مراحل إدارة المخاطر في البنوك

تمر عملية إدارة المخاطر بعدة مراحل رئيسية تهدف إلى تحليل وتقييم المخاطر ومعالجتها بفعالية داخل المؤسسات المالية، خاصةً في البنوك. وفقاً لمجموعة من الباحثين مثل (Girling ،Laycock (2014)، (2013)، (2016) Onyiriuba، (2016) Bellini، (2009) Gregoriou، (2006) Loader والمصادر الخاصة بالقطاع المصرفي الجزائري والدولي، يمكن تلخيص مراحل إدارة المخاطر كما يلي:

1.1 التعرف على المخاطر:

تُعد مرحلة التعرف على المخاطر خطوة أساسية في إطار إدارة المخاطر المصرفية، إذ تستلزم رصد وتحديد مختلف أنواع المخاطر التي قد تؤثر على سير العمليات، بما في ذلك المخاطر التشغيلية، الائتمانية، السوقية ومخاطر السيولة. وقد أكد (Laycock (2014 أن التحليل المنهجي للبيانات المالية والتقارير المصرفية يُسهم في الكشف المبكر عن المخاطر المحتملة. كما أشار (Mebarki (2022 و Benali إلى أهمية الاستناد إلى المعطيات المالية ومؤشرات السوق من أجل تحسين دقة تحديد هذه المخاطر. وفي السياق ذاته، شدد (BCBS (2011 على ضرورة تطوير أساليب معالجة وتحليل البيانات المرتبطة بالمخاطر التشغيلية والمالية لضمان تقييم أكثر فعالية.

2.1. تحليل وتقييم المخاطر:

بعد الانتهاء من تحديد المخاطر، تأتي مرحلة تحليلها وتقييم مدى خطورتها وتأثيرها المحتمل على البنك، وذلك من خلال دراسة احتمالية وقوع كل خطر وحجم أثره المالي. وقد بينَ (Bellini 2016) أن هذه المرحلة تعتمد على مجموعة من الأدوات مثل تحليل السيناريوهات، اختبارات التحمل، والنماذج الإحصائية. في هذا السياق، أكد (Hossain, Zarif (2020) أن تصنيف المخاطر إلى فئات محددة يسهم في تسهيل عملية التقييم، ويزيد من دقة النتائج وكفاءة اتخاذ القرار.

3.1. استراتيجيات التخفيف من المخاطر:

في هذه المرحلة، تُوضع خطط وإجراءات تهدف إلى تقليل المخاطر والحد من تأثيراتها على العمليات المصرفية. ويُعد تنوع المحافظ الاستثمارية من أبرز الوسائل المقترحة لتقليل المخاطر المالية، كما أوضح (Gregoriou 2009)، وذلك من خلال توزيع الاستثمارات لتقليل تأثيرها بتقلبات السوق. من جانبه، شدد (Loader 2006) على أهمية تعزيز أنظمة الرقابة الداخلية لضمان مراقبة سير العمليات المصرفية والحد من حالات الاحتيال. كما أشار (Onyiriuba 2016) إلى الدور المحوري لأدوات التحوط المالي وإدارة السيولة في التحكم بالمخاطر المالية. في السياق نفسه، بينَ (Agarwal و (Dhar 2014) أن استخدام التكنولوجيا الحديثة، مثل أنظمة الرقابة الإلكترونية، أصبح ضروريًا لمواجهة التهديدات السيبرانية المتزايدة. من جهة أخرى، اقترح (Hull 2018) اعتماد التأمين كوسيلة لتحمل المخاطر، حيث يُمكن أن يسهم في تقليل الأثر المالي الناتج عن المخاطر الجسيمة التي قد تواجه المؤسسات المالية.

كما أوضح (2020) De Roode و McCahery أن الاستعانة بجهات خارجية متخصصة في إدارة المخاطر يتيح للمؤسسات البنكية تعزيز فعالية استراتيجياتها من خلال الاستفادة من الخبرات المتخصصة وتطبيق مبادئ الحوكمة الرشيدة

4.1. تنفيذ خطط إدارة المخاطر:

تتطلب مرحلة تنفيذ استراتيجيات إدارة المخاطر تطبيق الإجراءات الوقائية وضمان فعاليتها ضمن العمليات المصرفية. وفي هذا السياق، أشار (2013) Girling إلى أن تحسين الهياكل التنظيمية والاستفادة من التكنولوجيا الحديثة يساهم في تعزيز سرعة الاستجابة تجاه المخاطر.

كما شدد Akinwumi و Ojo (2018) على أهمية تحقيق التكامل بين الأنظمة المالية والبنية التحتية التقنية لتحقيق تنفيذ فعال لاستراتيجيات إدارة المخاطر. من جانب آخر، أكد Khelifi , Bouras 2019 أن الالتزام بالمعايير المصرفية يُعد شرطاً أساسياً لضمان نجاح سياسات إدارة المخاطر، لا سيما في الدول النامية مثل الجزائر.

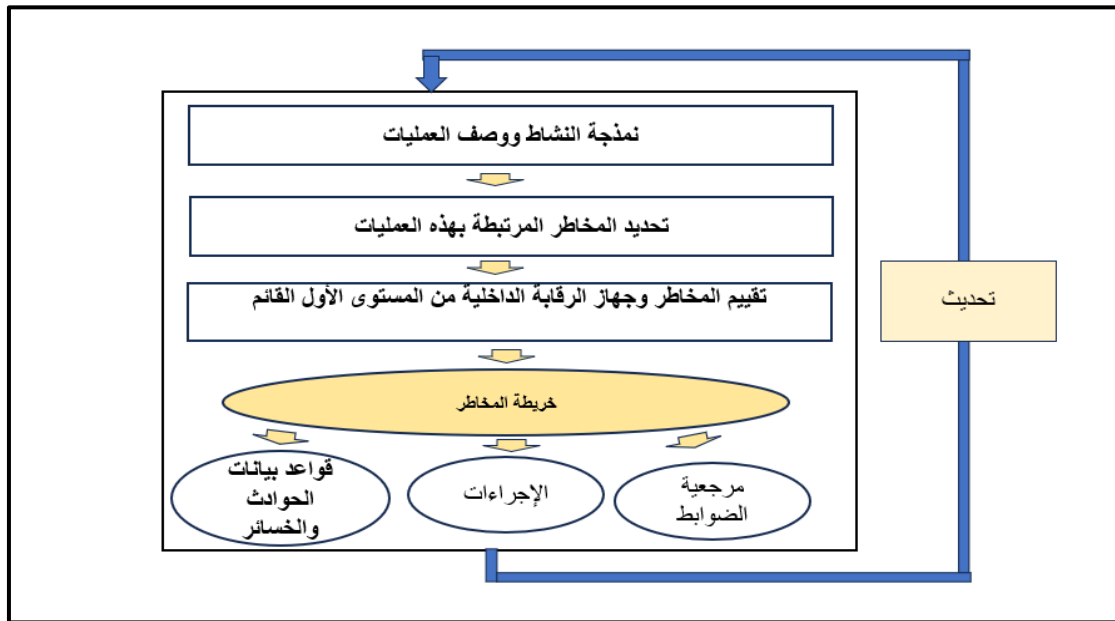
5.1. تتبع وتحديث المخاطر

تشكل عملية المتابعة المستمرة جزءاً لا يتجزأ من إدارة المخاطر، إذ تتطلب مراقبة دائمة لاستراتيجيات التخفيف وتقييم فعاليتها بشكل منتظم. وقد أكد (2009) Collier على ضرورة إدخال تعديلات دورية على هذه الاستراتيجيات بما يتوافق مع المتغيرات الاقتصادية والتشريعات المصرفية. وفي السياق نفسه، أشار Chenrobai ، Jorion و Yu (2010) إلى أن التطور المتسارع في حجم وتعقيد العمليات المصرفية يستدعي مراجعة دورية لسياسات إدارة المخاطر التشغيلية. وفي هذا الإطار، تُعد مؤشرات المخاطر الرئيسية (Key Risk Indicators - KRIs) أدوات أساسية في عملية التتبع، حيث تُستخدم كمقاييس لتحديد وتقييم المخاطر المحتملة التي قد تُعيق تحقيق أهداف المؤسسة

(Secureframe, 2024) وتعمل هذه المؤشرات كنظام إنذار مبكر يمكن المؤسسات من اتخاذ إجراءات استباقية للتقليل من المخاطر قبل تفاقمها (Secureframe, 2024) وفي السياق البنكي، تُستخدم KRIs لمراقبة المخاطر التشغيلية والاستراتيجية، كارتفاع معدلات الأخطاء أو زيادة عدد الشكاوى، مما يوفر رؤى دقيقة حول نقاط الضعف في نظم الرقابة والعمليات ومن خلال دمج هذه المؤشرات في إطار شامل لإدارة المخاطر، تتمكن المؤسسات المالية من تعزيز قدرتها على التنبؤ بالمخاطر المحتملة واتخاذ قرارات أكثر وعياً للحفاظ على استقرارها المالي والتشغيل

(Beasley, Branson, & Hancock, 2010)

الشكل 2: خطوات عملية إدارة المخاطر



المصدر: خلية إدارة المخاطر في تراست بنك

توضيح: الشكل يوضح المنهجية المتبعة من طرف بنك تراست في إدارة المخاطر

المطلب الرابع: التدقيق والرقابة الداخلية والتنظيم الاحترافي لمنظومة إدارة لمخاطر

1. التدقيق والرقابة الداخلية لمنظومة إدارة لمخاطر:

تُعد المخاطر المصرفية من أبرز التحديات التي تواجه البنوك مما يستوجب وجود آليات فعّالة لضبطها والحد من آثارها في هذا السياق يبرز دور كل من التدقيق الداخلي والرقابة الداخلية كوسيلتين أساسيتين لضمان سلامة العمليات المصرفية وكفاءة إدارة المخاطر ويساعد على فهم هذين المفهومين في تعزيز الشفافية وتحقيق الانضباط داخل المؤسسات البنكية.

1.1. تعريف الرقابة الداخلية:

تعد الرقابة الداخلية من العناصر الأساسية التي تساهم في ضمان استقرار وكفاءة أداء المنظمة فهي تمثل مجموعة من الإجراءات والسياسات التي تهدف إلى تحقيق الأهداف التشغيلية، والحفاظ على الأصول، وضمان الالتزام بالقوانين والمعايير.

ووفقاً للجنة بازل للإشراف المصرفي (2019) تعتبر الرقابة الداخلية أداة حيوية لتعزيز الامتثال وتقليل التعرض للمخاطر من خلال نظام مراقبة داخلي فعال ومستقل (BCBS, 2019). كما يصف COSO (2013) إطار عمل الرقابة الداخلية بأنها نظام متكامل يهدف إلى تعزيز الحوكمة وضمان الامتثال للوائح القانونية، وتحقيق الكفاءة التشغيلية داخل المصارف (COSO, 2013). بحسب دراسة Bourke (2018)، تمثل الرقابة الداخلية المصرفية مجموعة من الإجراءات التي تهدف إلى حماية أصول البنك، وتحقيق دقة التقارير المالية، وضمان الامتثال للمتطلبات التنظيمية (Bourke, 2018).

يؤكد تقرير Deloitte (2020) أن الرقابة الداخلية في البنوك تلعب دوراً أساسياً في إدارة المخاطر وتوفير رؤية واضحة حول الأداء المالي مما يعزز الثقة بين المستثمرين وأصحاب المصالح (Deloitte, 2020).

انطلاقاً من التعاريف السابقة يمكننا أن نلاحظ أن هناك اتفاقاً بين الباحثين والهيئات الرقابية على أن الرقابة الداخلية تُعد عنصرًا أساسيًا ضمن البنية التنظيمية للمؤسسات المالية حيث تُساهم في تعزيز الحوكمة وضمان حماية الأصول والامتثال للتشريعات التنظيمية إلى جانب ضمان دقة وموثوقية التقارير المالية كما يُنظر إلى الرقابة الداخلية على أنها أداة ديناميكية ينبغي أن تكون قادرة على التكيف مع التغيرات المحيطة سواء كانت تكنولوجية أو تنظيمية بما يُمكن البنوك من مواجهة المخاطر المتزايدة خصوصاً في بيئة مالية تتسم بعدم اليقين.

كما تبرز الرقابة الداخلية بوصفها إطاراً فعالاً لإدارة المخاطر فهي لا تقتصر على مجرد مراقبة الامتثال بل تسهم في تحقيق رؤية واضحة للأداء المالي والتشغيلي مما يعزز الثقة لدى أصحاب المصالح ويحدّ من فرص التعرض للانحرافات والاختلالات التشغيلية.

وبناءً على ما سبق يمكننا اقتراح تعريف تركيبي للرقابة الداخلية المصرفية على النحو التالي:

الرقابة الداخلية المصرفية، كهيئة مستقلة، هي نظام متكامل من الآليات والسياسات والإجراءات المصممة لضمان سلامة العمليات البنكية حماية الأصول، الالتزام باللوائح التنظيمية وتحقيق الشفافية والدقة في التقارير المالية مع توفير دعم فعال لعمليات إدارة المخاطر داخل البنك وتتميز هذه الرقابة بكونها مرنة وتكيفية تسعى إلى مواكبة التحولات التكنولوجية والتشريعية بما يُعزز من كفاءة الأداء ويضمن استمرارية العمال في بيئة مصرفية معقدة وديناميكية.

2.1. أهداف الرقابة الداخلية المصرفية:

تعد الرقابة الداخلية المصرفية أداة حيوية لضمان استقرار وكفاءة العمليات المصرفية فهي تهدف إلى تحقيق مجموعة من الأهداف الأساسية التي تساهم في حماية الأصول، تعزيز الامتثال، وتحقيق الكفاءة التشغيلية ومن بين هذه الأهداف نذكر الأهداف التالية:

– **ضمان الالتزام بالقوانين والتنظيمات:**

تُسهّم الرقابة الداخلية في التأكد من مطابقة العمليات البنكية للقوانين المالية والتنظيمات المعمول بها، ما يعزز من الامتثال المؤسسي. (المادة 105 من القانون رقم 09-23 (2023))

– **الكشف المبكر عن المخاطر والتهديدات:**

تهدف إلى تحديد وتقييم وإدارة مختلف أنواع المخاطر، بما فيها مخاطر التشغيل والائتمان، لتفادي الانحرافات قبل وقوعها. (المادة 106 من القانون رقم 09-23 (2023))

– **تعزيز الحوكمة والشفافية داخل المؤسسات البنكية:**

من خلال تكريس نظام الحوكمة وتحديد المسؤوليات، ما يسمح برقابة أكثر نجاعة وتوزيع واضح للمهام. (المادة 107 من القانون رقم 09-23 (2023))

– **تحسين فعالية الرقابة والإشراف الداخلي:**

اعتماد أنظمة رقابة داخلية مستقلة وفعالة لضمان السيطرة على العمليات البنكية وتقييم الأداء باستمرار. (المادة 108 من القانون رقم 09-23 (2023))

– **الوقاية من تبييض الأموال وتمويل الإرهاب:**

من خلال وضع آليات دقيقة لرصد المعاملات المشبوهة، والإبلاغ عنها، وفق ما تفرضه المعايير الدولية. (المادة 5 من النظام رقم 03-24 (2024))

– **حماية أصول البنك وموارده المالية:**

تهدف إلى تجنب الخسائر الناتجة عن التلاعب أو الأخطاء، من خلال ضمان تأمين كافٍ على الأصول والممتلكات. (المادة 110 من القانون رقم 09-23 (2023))

– تعزيز كفاءة الأداء وضمان استمرارية النشاط البنكي:

تساهم الرقابة في تحسين سير العمليات البنكية اليومية وزيادة الفعالية والاستجابة للأزمات.

(المادة 111 من القانون رقم 23-09 (2023))

كما تم الإشارة أيضا إلى أهداف الرقابة الداخلية المصرفية من طرف بعض من الهيئات والباحثين وهي كالتالي:

– حماية أصول البنك:

تهدف الرقابة الداخلية إلى حماية أصول المؤسسة المالية من الاحتيال وسوء الاستخدام، والخسائر غير المتوقعة، من خلال وضع سياسات صارمة للرقابة والمتابعة (BCBS, 2011).

– تحقيق الامتثال للقوانين واللوائح: تهدف إلى ضمان التزام البنوك بالقوانين المالية والتنظيمية

المعمول بها مما يقلل من المخاطر القانونية والعقوبات (COSO, 2013).

– ضمان دقة التقارير المالية: تساعد الرقابة الداخلية في ضمان أن السجلات المالية تعكس

الواقع بدقة، مما يدعم قرارات الإدارة والمساهمين (Deloitte, 2020).

– تحسين الكفاءة التشغيلية:

تعزز العمليات الداخلية الفعالة من الأداء المؤسسي، مما يسهم في تحقيق الأهداف الاستراتيجية

وتقليل الهدر المالي والإداري (Bourke, 2018).

– تعزيز الثقة والشفافية:

تساهم في تحسين ثقة العملاء والمستثمرين من خلال ضمان وجود نظام رقابي قوي يقلل من

التلاعب والفساد. (قانون رقم 06-01 المؤرخ في 20 فيفري 2006، المادة 9)

2. مكونات الرقابة الداخلية المصرفية:

بناءً على التنظيم الخاص ببنك الجزائر، وتحديداً التنظيم رقم 08-2011 المؤرخ في 28 نوفمبر

2011 المتعلق بالرقابة الداخلية للبنوك والمؤسسات المالية، يمكن تصنيف مكونات نظام الرقابة الداخلية المصرفية كما يلي:

- نظام مراقبة العمليات والإجراءات الداخلية: (Règlement n°2011-08 Art 4)

يتضمن وضع آليات رقابية لمتابعة تنفيذ العمليات المصرفية وفقاً للسياسات والإجراءات المعتمدة، بهدف الحد من المخاطر التشغيلية وتعزيز الامتثال التنظيمي.

- التنظيم المحاسبي ومعالجة البيانات المالية:

يشمل تطبيق أنظمة محاسبية دقيقة ومعايير شفافة لمعالجة البيانات المالية، مما يعزز موثوقية التقارير المالية ويضمن الامتثال للمتطلبات الرقابية. (Règlement n°2011-08 Art 4)

- أنظمة قياس المخاطر وتقييم الأداء: (Regalement n°2011-08, Art. 37-53)

تعتمد على مجموعة من الأدوات والتقنيات المستخدمة لتحديد المخاطر المحتملة وتقييمها، مما يساهم في تحسين آليات اتخاذ القرار وتقليل احتمالية التعرض لمخاطر مالية وتشغيلية.

- إجراءات الرقابة وإدارة المخاطر:

تتضمن تطوير أنظمة فعالة لمراقبة المخاطر المصرفية، مع تعزيز عمليات التدقيق الداخلي لضمان الامتثال للضوابط الرقابية وتحقيق الكفاءة التشغيلية (Règlement n°2011-08, Art. 4)

- نظام التوثيق والأرشفة: (Règlement n°2011-08, Art. 4)

يهدف إلى توفير إطار متكامل لتوثيق العمليات المصرفية وحفظ السجلات بطريقة تسهل عملية المراجعة والتدقيق، مع ضمان الامتثال لمتطلبات الشفافية والرقابة الداخلية.

– قواعد الحوكمة والرقابة المؤسسية: (Règlement n°2011-08, Art. 9)

تشمل تحديد مسؤوليات الجهات الرقابية والإدارية داخل البنك، مثل مجلس الإدارة ولجنة التدقيق ولجنة المخاطر، لضمان الالتزام بالممارسات الرشيدة في الإدارة والرقابة الداخلية.

3. مبادئ الحوكمة والرقابة البنكية:

تُعد مبادئ الحوكمة الصادرة عن لجنة بازل (2015) إطارًا مرجعيًا دوليًا يهدف إلى تعزيز فعالية الرقابة الداخلية في البنوك، من خلال 13 مبدأ 9:47 ص 9:47 ص 9:47 صاً لضمان الشفافية، الاستقلالية، وإدارة المخاطر بشكل منهجي ومدروس. وفيما يلي شرحها:

مبدأ 1 – المسؤوليات العامة لمجلس الإدارة: (BCBS, 2015)

يتحمل مجلس الإدارة المسؤولية الشاملة عن الإشراف على الشؤون العامة للبنك، بما يشمل تحديد القيم المؤسسية، استراتيجية الأعمال، الإشراف على الإدارة العليا، وثقافة المخاطر.

مبدأ 2 – تكوين مجلس الإدارة ومؤهلاته:

يجب أن يكون مجلس الإدارة مكوناً من أعضاء ذوي مؤهلات وخبرات متنوعة تضمن فعالية الإشراف كما يجب أن تشمل العملية معايير لاختيار الأعضاء ومراقبة أدائه (BCBS, 2015)

مبدأ 3 – هيكل وممارسات مجلس الإدارة:

يجب أن تكون للمجلس هياكل فعالة مثل فصل دور الرئيس التنفيذي ورئيس المجلس، وإنشاء لجان متخصصة (كالتدقيق وإدارة المخاطر) لضمان أداء مهامه بكفاءة (BCBS, 2015).

مبدأ 4 – الإدارة التنفيذية:

يجب أن تضمن الإدارة التنفيذية التنفيذ اليومي لاستراتيجية البنك بطريقة تتماشى مع السياسة المعتمدة من المجلس وقيم البنك (BCBS, 2015).

مبدأ 5-حوكمة المجموعات المصرفية:

في حالة المجموعات المصرفية، يجب أن يضمن مجلس إدارة الشركة الأم وجود سياسات مناسبة للحوكمة تغطي المجموعة بأكملها بما في ذلك الفروع والشركات التابعة (BCBS, 2015) .

مبدأ 6-وظيفة إدارة المخاطر:

يجب أن يكون للبنك وظيفة مستقلة لإدارة المخاطر بقيادة مسؤول رئيسي عن المخاطر (CRO)، مع الصلاحيات الكافية للوصول إلى المجلس مباشرة عند الضرورة (BCBS, 2015) .

مبدأ 7-كشف ومراقبة ومتابعة المخاطر:

يجب أن يكون لدى البنك نظام قوي لرصد وتحديد المخاطر في الوقت المناسب على جميع مستويات المؤسسة، واتخاذ الإجراءات اللازمة لإدارتها (BCBS, 2015) .

مبدأ 8-الاتصال والإبلاغ بالمسائل المخاطر:

ينبغي أن تضمن البنوك أن يتم الإبلاغ عن المعلومات المتعلقة بالمخاطر بطريقة دقيقة، شاملة وفي الوقت المناسب لمجلس الإدارة والإدارة العليا (BCBS, 2015) .

مبدأ 9-الالتزام بالقوانين والأنظمة:

يجب أن يكون للبنك وظيفة امتثال مستقلة، تضمن الالتزام بالقوانين والتشريعات المعمول بها والسياسات الداخلية (BCBS, 2015) .

مبدأ 10-التدقيق الداخلي:

يجب أن تكون هناك وظيفة تدقيق داخلي فعالة ومستقلة تقدم تأكيدات موضوعية بشأن كفاءة وفعالية الحوكمة والضوابط الداخلية للبنك (BCBS, 2015) .

مبدأ 11-سياسة المكافآت:

يجب أن تدعم نظم التعويضات ثقافة المخاطر السليمة والحوكمة الجيدة، وأن تربط المكافآت بالأداء المستدام والمتحفظ في تحمل المخاطر (BCBS, 2015).

مبدأ 12-المعلومات والشفافية:

ينبغي أن توفر البنوك معلومات دقيقة وفي الوقت المناسب للمساهمين وأصحاب المصالح الآخرين لضمان الرقابة والمساءلة الفعالة (BCBS, 2015).

مبدأ 13-دور السلطات الرقابية:

على السلطات الرقابية وضع إرشادات للحوكمة، ومراقبة امتثال البنوك لها، وفرض التحسينات والتدخل عند الحاجة لضمان الحوكمة السليمة (BCBS, 2015).

تعتمد إدارة المخاطر البنكية على كل هذه المبادئ التي تهدف إلى تعزيز الاستقرار المالي حيث نعتمد في إدارة المخاطر على ثلاثة مبادئ رئيسية وهي المبادئ 6 و7 و8

في هذا السياق ووفقاً لمبادئ بازل الخاصة بالحوكمة (رقم 1-2-3 و4)، بنك الجزائر أصدر النظام رقم 01-25 المؤرخ في 22 أبريل 2025، الذي يحدد شروط اعتماد مديري البنوك، وهي:

- ضمان كفاءتهم (مهاراتهم ونزاهتهم) للحفاظ على استقرار النظام المصرفي.
- متطلبات الموافقة: يجب على أي شخص يتم تعيينه كمدير أن يحصل على موافقة مسبقة من محافظ بنك الجزائر (المادة 4).
- يجب تقديم طلب الموافقة خلال 15 يوماً من تاريخ التعيين (المادة 5).

- الشرف: عدم وجود أحكام جنائية أو عقوبات تأديبية أو ارتباطات بكيانات إرهابية أو تضارب في المصالح (المادة 7).

- المهارات: الشهادات الجامعية (المصرفية/التمويل)، الخبرة المهنية ذات الصلة، القدرة الكافية على القيام بالمهام (المادة 7).

4. أنظمة إدارة المخاطر في المنظومة البنكية الجزائرية:

وفقاً لما ورد في التنظيم رقم 11-08 المؤرخ في 28 جوان 2011 المتعلق بنظام الرقابة الداخلية للبنوك والمؤسسات المالية، فإن هذا التنظيم يحدد بدقة الأنظمة الأساسية للرقابة التي يجب أن تتوفر لدى كل بنك أو مؤسسة مالية لضمان الامتثال، الحد من المخاطر، وتعزيز الاستقرار المالي أنظمة الرقابة الواجب توفرها وفقاً للتنظيم 11-08:

1.4. نظام الرقابة الداخلية العامة: (المادة 5)

يهدف إلى التحكم في العمليات وضمان امتثالها للتشريعات، ويشمل جميع المستويات التنظيمية للبنك

2.4. نظام الرقابة على الامتثال:

يتوجب على كل بنك إنشاء وظيفة مستقلة للامتثال تكون مكلفة بمراقبة مدى احترام القوانين والتنظيمات السارية والتعليمات الداخلية (المادتان 11 و12)

3.4. نظام إدارة المخاطر:

يشمل آليات لتحديد، تقييم، ومراقبة كافة أنواع المخاطر (الائتمانية، التشغيلية، السوق، السيولة...)

ويجب أن يكون مستقلاً عن وظائف التنفيذ (المواد 19 إلى 23)

4.4. نظام الرقابة المحاسبية والمعلوماتية:

يجب على البنك التأكد من موثوقية نظامه المحاسبي والمعلوماتي، والتكفل بجودة البيانات وتناسقها وسلامتها (. المادتان 25 و26)

5.4. نظام الرقابة على المخاطر الائتمانية: (المواد 27 و28)

يجب وجود نظام لتقييم ومراقبة مخاطر منح القروض، يعتمد على تصنيف الزبائن وتحليل الضمانات.

6.4. نظام مراقبة الالتزامات الكبرى: (المادة 29)

يفرض على البنوك مراقبة احترام الحدود القصوى للالتزامات تجاه العملاء أو المجموعات الاقتصادية.

7.4. نظام إدارة السيولة: (المادة 30)

يجب وضع آليات لتقدير احتياجات السيولة الفورية والمستقبلية وضمان التوازن بين الأصول والخصوم

8.4. نظام إدارة العمليات الحساسة والخاصة: (المادتان 31 و32)

يتوجب على البنوك تحديد ومراقبة العمليات الحساسة أو غير العادية والتحقق من مشروعيتها.

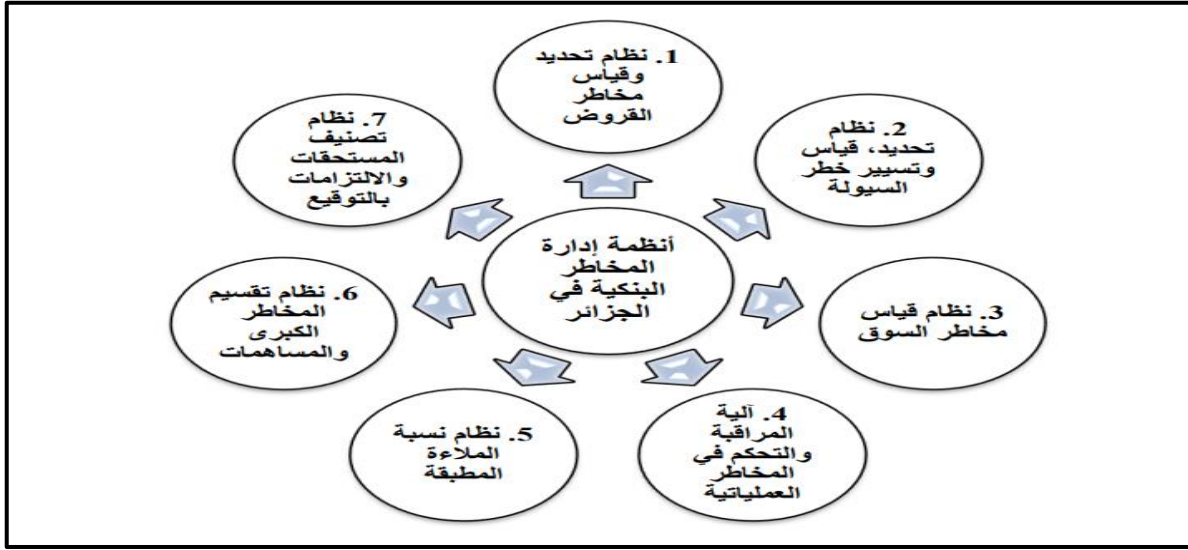
9.4. نظام الرقابة على أمن المعلومات والمعطيات: (المادة 33)

يجب على المؤسسة وضع وسائل لضمان سرية وسلامة الأنظمة المعلوماتية والبيانات

10.4. نظام التدقيق الداخلي :

وظيفة مستقلة تقوم بتقييم مدى فعالية أنظمة الرقابة، وتقديم توصيات للإدارة (المواد 4 و45)

الشكل 3: أنظمة إدارة المخاطر البنكية في المنظومة البنكية الجزائرية



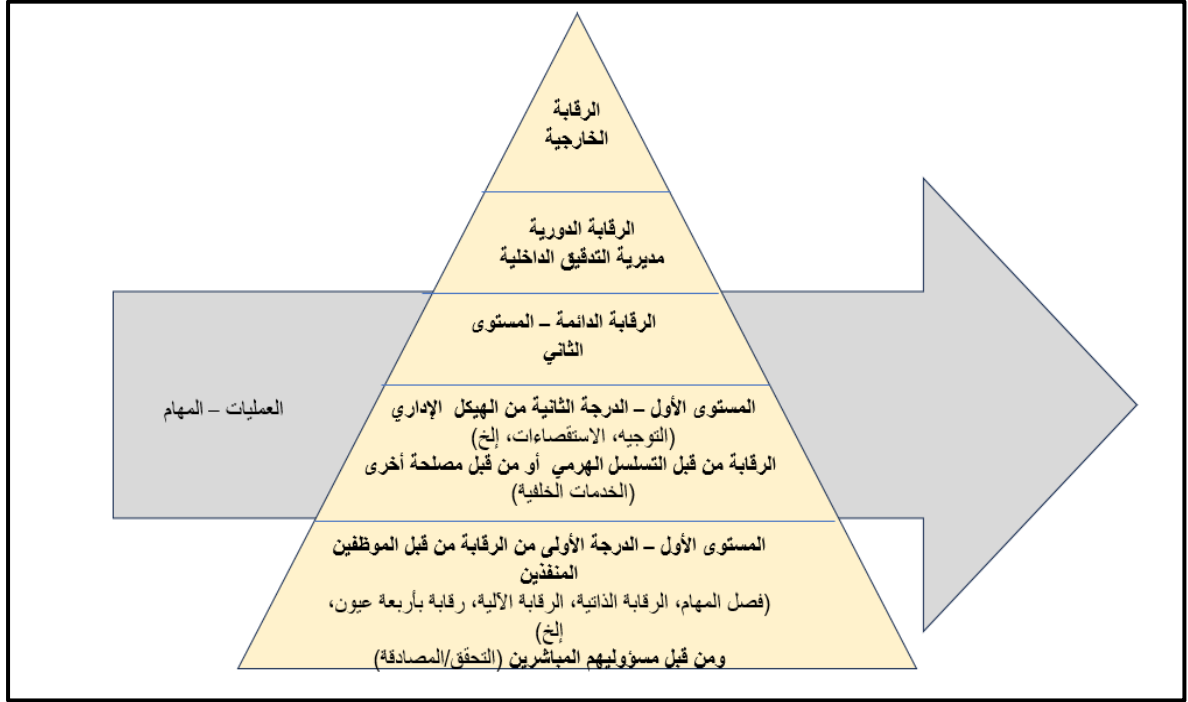
المصدر: فياش، آ.، مباني، ع. ا. (2017) أنظمة وآليات إدارة المخاطر البنكية في الجزائر: دراسة

حالة بنك الإسكان للتجارة والتمويل/الجزائر (2010-2017). جامعة الجزائر

5. الرقابة الداخلية وإدارة المخاطر المصرفية:

من أجل تعزيز فعالية الرقابة على العمليات والمهام داخل المؤسسة، يتم اعتماد نظام رقابي متدرج يقوم على عدة مستويات، يهدف إلى ضمان تنفيذ المهام بكفاءة واكتشاف الانحرافات مبكرًا. ويُبرز هذا النظام دور كل من الموظفين، والإدارة، والجهات المستقلة في دعم الرقابة الداخلية والخارجية. يوضح الشكل التالي الهيكل الهرمية للرقابة بأنواعها المختلفة، بدءًا من الرقابة الذاتية التي يمارسها الموظفون أنفسهم، مرورًا بالرقابة الإدارية الداخلية، وصولًا إلى الرقابة الدورية والخارجية التي تقوم بها أطراف مستقلة. ويساهم هذا التدرج في توزيع المسؤوليات الرقابية بشكل متكامل يعزز من فعالية نظام الرقابة الشامل.

الشكل 4: مستويات الرقابة على المخاطر البنكية



المصدر: مديرية الرقابة في بنك ترست

6. دور الرقابة الداخلية في إدارة المخاطر المصرفية:

تساهم الرقابة الداخلية في تحديد المخاطر المحتملة التي تواجه البنوك من خلال مراقبة الأنشطة التشغيلية وضمان الامتثال للمعايير التنظيمية. ووفقاً للجنة بازل، يعتمد النظام الفعال للرقابة الداخلية على مبادئ تشمل إشراف الإدارة، وتحديد وتقييم المخاطر، وتنفيذ أنشطة رقابية مناسبة، وتوفير المعلومات والتواصل الفعال، بالإضافة إلى المتابعة والتقييم المستمر لضمان فعالية النظام الرقابي.

(BCBS, 2011)

7. التكامل بين الرقابة الداخلية وإدارة المخاطر:

تُعتبر الرقابة الداخلية وإدارة المخاطر في البنوك نظامين مترابطين يعملان على تعزيز الاستقرار المالي. فالرقابة الداخلية تُسهم في تحديد وتقييم المخاطر المحتملة، مثل المخاطر الائتمانية والتشغيلية ومخاطر السوق، من خلال مراقبة الأنشطة التشغيلية وضمان الامتثال للمعايير التنظيمية. من جانبها، تعتمد

إدارة المخاطر على نظام رقابة داخلية قوي لتوفير معلومات دقيقة وموثوقة تُسهم في اتخاذ قرارات مستنيرة بشأن إدارة المخاطر. وقد أكدت لجنة بازل للرقابة المصرفية على أهمية هذا التكامل، حيث أشارت إلى أن "البنوك يجب أن تطور وتنفذ وتحافظ على إطار لإدارة المخاطر التشغيلية يكون مدمجًا بالكامل في عمليات إدارة المخاطر العامة للبنك (BCBS, 2011).

8. أثر الرقابة الداخلية على استقرار النظام المصرفي: (BCBS, 2011).

أكدت الدراسات أن وجود آليات رقابة داخلية قوية يحدّ من الخسائر المالية ويحسّن الشفافية ويضمن امتثال المؤسسات المصرفية للمعايير الدولية مثل توصيات لجنة بازل حول الرقابة المصرفية وتدعو هذه التوصيات إلى دمج الممارسات الرقابية في عملية إدارة المخاطر من خلال تعزيز الضوابط الداخلية وآليات المراقبة المستمرة (Koudri, 2022).

9. إدارة المخاطر والتنظيم الاحترازي

تهدف إدارة المخاطر والتنظيم الاحترازي إلى تعزيز استقرار النظام المالي وضمان الامتثال للمعايير الدولية والمحلية المعتمدة في القطاع المصرفي. تعمل الجهات التنظيمية، مثل لجنة بازل وبنك الجزائر، على وضع معايير تحدد متطلبات رأس المال والضوابط الاحترازية لمواجهة المخاطر المحتملة التي تواجه المؤسسات المالية (Zaafrane, 2016).

1.9. اتفاقيات بازل 1 (1988): شكلت اتفاقية بازل الأولى أول إطار تنظيمي عالمي يحدد الحد الأدنى لمتطلبات رأس المال للمصارف، حيث فرضت نسبة 8% كحد أدنى للأموال الخاصة الفعلية مقارنة بإجمالي الأصول المرجحة بالمخاطر، مما عزز من قدرة البنوك على مواجهة المخاطر المالية المختلفة (BCBS, 1988).

2.9. اتفاقيات بازل II (2005)

جاءت اتفاقية بازل الثانية لمعالجة أوجه القصور في الاتفاقية الأولى، من خلال إضافة ثلاثة أركان رئيسية لإدارة المخاطر:

الركيزة الأولى: تتعلق بحساب الحد الأدنى لمتطلبات رأس المال لمواجهة المخاطر الائتمانية، مخاطر السوق، والمخاطر التشغيلية.

الركيزة الثانية: تعنى بالإشراف والرقابة المصرفية لتعزيز الامتثال لمتطلبات رأس المال والمخاطر.

الركيزة الثالثة: تركز على متطلبات الإفصاح لتعزيز الشفافية المالية للمؤسسات المصرفية

3.9. اتفاقيات بازل III (2011)

جاءت اتفاقية بازل الثالثة كرد فعل للأزمة المالية العالمية التي حدثت في عام 2008، بهدف تعزيز قدرة النظام المصرفي على مواجهة الأزمات المالية وتحسين إدارة المخاطر بشكل عام. وعلى الرغم من أن اتفاقية بازل الثالثة احتفظت بالركائز الثلاث من اتفاقية بازل الثانية، إلا أنها أضافت تحسينات جوهرية تمثلت في:

– **الركيزة الأولى:** تعزيز جودة وهيكلة رأس المال من خلال التركيز على رأس المال الأساسي (Core Tier 1) وزيادة الحد الأدنى لنسبة كفاية رأس المال، مع الأخذ في الاعتبار إضافة مخاطر جديدة مثل مخاطر السيولة والرفع المالي.

– **الركيزة الثانية:** تحسين أدوات الرقابة والإشراف المصرفي من خلال التأكيد على أهمية فعالية إدارة المخاطر والحوكمة داخل البنوك.

– **الركيزة الثالثة:** تعزيز متطلبات الإفصاح والشفافية، مما يضمن أن يكون لدى جميع أصحاب المصلحة إمكانية الوصول إلى معلومات دقيقة حول مستويات رأس المال والمخاطر داخل المؤسسات المصرفية. (BCBS, 2011)

4.9. التنظيم الاحترازي على المستوى الوطني:

على المستوى الوطني، أصدر بنك الجزائر لوائح تنظيمية مثل التنظيم رقم 11-08 لعام 2011 المتعلقة بالرقابة الداخلية في البنوك والمؤسسات المالية، والذي حدد الإطار العام للرقابة الداخلية وإدارة المخاطر.

كما عزز القانون رقم 14-01 من متطلبات الإفصاح عن نسب الملائمة المالية لضمان الامتثال للمعايير الاحترازية الدولية. (Banque d'Algérie, 2011; Banque d'Algérie, 2014)

لتوضيح التنظيم الاحترازي على المستوى الوطني في الجزائر المتعلقة بتسيير المخاطر، يمكن الرجوع إلى التشريعات الوطنية، وخصوصًا تلك المتعلقة بالبنك المركزي الجزائري

(Banque d'Algérie) يتعامل هذا التنظيم مع المبادئ التي تطرقت لها لجنة بازل، مع تخصيص مواد قانونية وإجرائية تسعى لضمان استقرار النظام المالي ويمكن تلخيصها في المواد القانونية التالية:

إدارة المخاطر: وفقًا للمادة 3 من التنظيم رقم 11-08 المتعلقة بنظام الرقابة المصرفية، يجب على المؤسسات المالية أن تقوم بتحديد وتصنيف المخاطر التي قد تواجهها في إطار سياسات عامة لإدارة

المخاطر (d'Algérie, 2011 Banque)

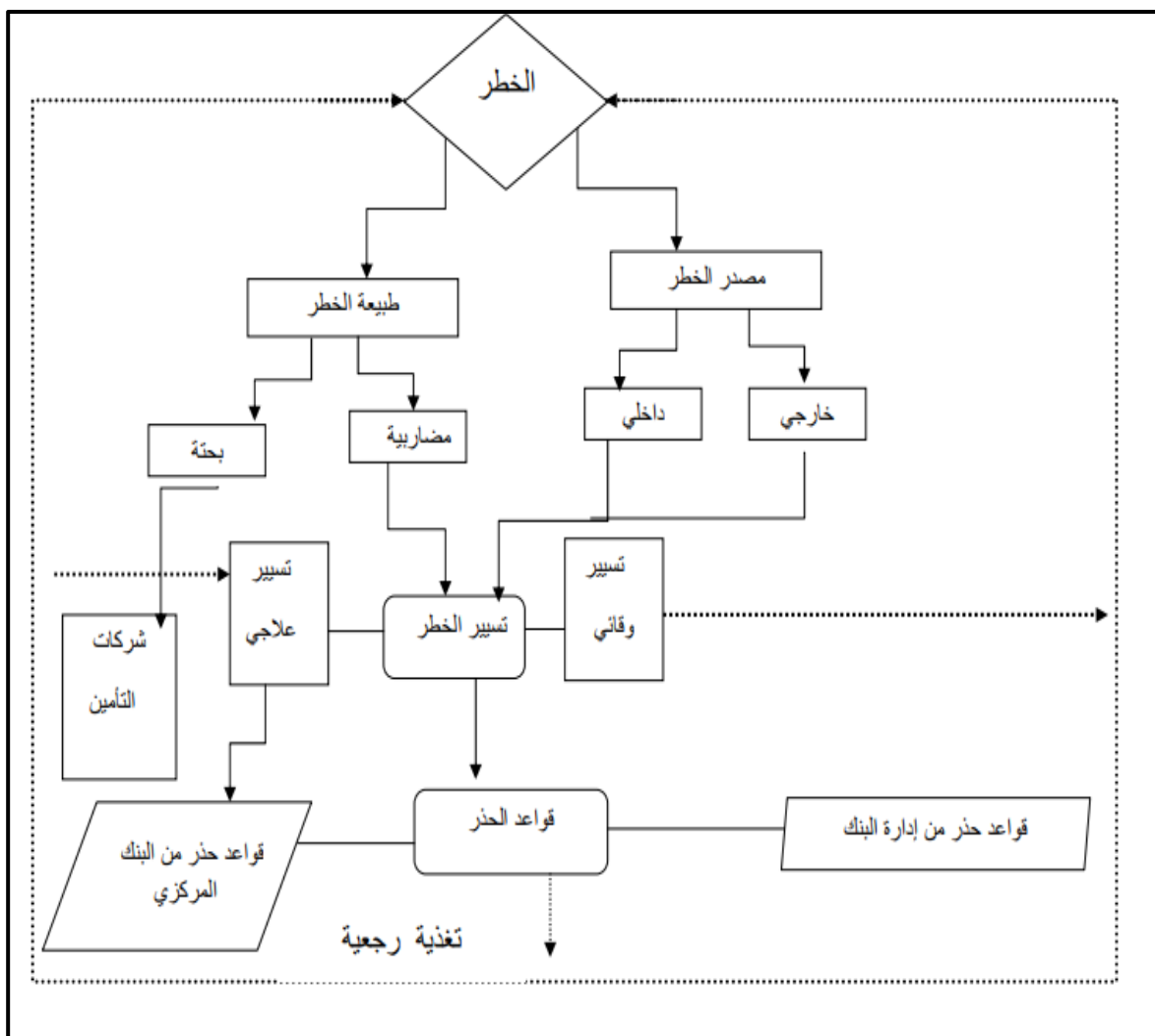
هذه السياسة يجب أن تشمل المخاطر الائتمانية، التشغيلية، والمخاطر المرتبطة بالسيولة.

الرقابة الداخلية الفعالة: المادة 5 من نفس التنظيم تتطلب أن تمتلك البنوك أنظمة رقابية داخلية لضمان الامتثال للقوانين والأنظمة السارية، مما يعزز القدرة على التحكم في المخاطر المالية والتشغيلية (Banque d'Algérie, 2011)

الإفصاح والشفافية: طبقاً للمادة 6 من التنظيم رقم 11-08، تتطلب التشريعات الجزائرية من المؤسسات المالية الإفصاح عن مستويات رأس المال والمخاطر، ما يساهم في بناء الثقة مع المتعاملين والسلطات الرقابية (Banque d'Algérie, 2011)

الامتثال والتقارير: المادة 7 تشير إلى ضرورة أن تقوم المؤسسات المالية بتقديم تقارير دورية حول تقييمات المخاطر وإجراءات الرقابة التي تتخذها لضمان الامتثال للمتطلبات الرقابية في إطار الأنظمة المالية المحلية والدولية.

الشكل 5: تسيير الخطر والتنظيم الاحترازي



المصدر: رحيم حسين الاقتصاد المصرفي (مفاهيم تحاليل، تقنيات) دار بهاء الدين للنشر والتوزيع، الطبعة

الأولى، قسنطينة، 2008.

10. الإطار التنظيمي الجزائري المتعلق بتسيير المخاطر:

ينص القانون رقم 23-09 الصادر بتاريخ 21 جوان 2023 المتعلق بالنظام النقدي والمصرفي في الجزائر في مواده من 107 إلى 109 على مجموعة من الأحكام الهادفة إلى تعزيز الحوكمة وتسيير المخاطر داخل البنوك.

تُفرض على البنوك وضع قواعد داخلية للحوكمة تُحدد بوضوح صلاحيات ومسؤوليات كل من مجلس الإدارة والإدارة العامة كما يتوجب عليها إنشاء منظومة فعالة للرقابة الداخلية تتضمن عمليات وهياكل تنظيمية داخلية تضمن:

- السير الحسن والفعال للعمليات المصرفية
- موثوقية ودقة المعلومات المالية
- سلامة وأمن الأصول.

ويشترط أن تكون هذه المنظومة متناسبة مع طبيعة وحجم الأنشطة البنكية وعدد الفروع، وانتشارها الجغرافي بما يمكن من تحديد المخاطر المختلفة وقياسها والحد من آثارها.

وفي هذا السياق أصدر بنك الجزائر بناءً على هذا القانون وما سبقه من نصوص جملة من التنظيمات والتعليمات التي تهدف إلى ضبط وتوجيه مراقبة وتسيير المخاطر المصرفية من بينها:

- التنظيم رقم 91-09 المؤرخ في 14 أوت 1991 المعدل والمتمم المتعلق بالقواعد الاحترازية لتسيير البنوك والمؤسسات المالية
- التنظيم رقم 05-05 المؤرخ في 15 ديسمبر 2005 الخاص بالوقاية من تبييض الأموال وتمويل الإرهاب والذي استبدل مؤخرًا بالتنظيم رقم 24-03 بتاريخ 24 جويلية 2024.

- التنظيم رقم 05-09 المؤرخ في 18 أكتوبر 2009، المتعلق بإعداد ونشر البيانات المالية للبنوك
- التنظيم رقم 08-09 المؤرخ في 29 ديسمبر 2009 حول تقييم وتسجيل الأدوات المالية
- التنظيم رقم 03-11 المؤرخ في 24 ماي 2011 بخصوص مراقبة المخاطر بين البنوك
- التنظيم رقم 04-11 المؤرخ في 24 ماي 2011 المتعلق بتحديد وقياس وتسيير ومراقبة مخاطر السيولة
- التنظيم رقم 01-2014 الصادر في 16 فيفري 2014 حول نسب الملاءة المالية للبنوك
- التنظيم رقم 02-2014 المؤرخ في 16 فيفري 2014 المتعلق بالمخاطر الكبرى والمساهمات.
- التعليم رقم 01-25 المؤرخة في 22 أبريل 2025 المتعلقة بالاعتماد (الموافقة الرسمية) الخاص بالمديرين التنفيذيين وأعضاء مجالس إدارة البنوك.

المبحث الثالث: خارطة المخاطر البنكية

تواجه البنوك مجموعة متنوعة من المخاطر التي قد تؤثر على استقرارها المالي وسمعتها مما يتطلب أسلوبًا منهجيًا لتحديد هذه المخاطر وتحليلها وتعد خارطة المخاطر البنكية أداة استراتيجية تسهم في تصنيف المخاطر وتقدير احتمالية حدوثها وتأثيرها مما يساعد الإدارة على اتخاذ قرارات استباقية وتعزيز فعالية إدارة المخاطر داخل المؤسسة المصرفية.

المطلب الأول: عموميات حول خارطة المخاطر البنكية

1. مفهوم خارطة المخاطر البنكية:

تعد خارطة المخاطر البنكية أداة حيوية في إدارة المخاطر داخل المؤسسات المصرفية حيث تساعد البنوك على تحديد وتصنيف المخاطر المحتملة التي قد تؤثر على عملياتها وأدائها من خلال تحليل هذه المخاطر تتمكن البنوك من وضع استراتيجيات وقائية فعّالة للتقليل من تأثيراتها السلبية سنستعرض في هذا السياق مجموعة من التعاريف التي توضح مفهوم خارطة المخاطر البنكية وأهميتها في سياق العمل المصرفي.

1.1 من منظور تكنولوجي: (Agarwal & Dhar, 2014):

خارطة المخاطر التشغيلية هي أداة تحليلية تُستخدم لتحديد المخاطر الناجمة عن التكنولوجيا الحديثة بما في ذلك الأعطال التقنية والهجمات الإلكترونية، مما يساعد المؤسسات المالية على تعزيز الأمن السيبراني وإدارة المخاطر بفعالية.

2.1. من منظور الامتثال التنظيمي: (BCBS, 2011):.

تمثل خارطة المخاطر التشغيلية إطارًا متكاملًا يساعد البنوك على تقييم مدى التزامها بالمعايير التنظيمية الوطنية والدولية، مثل اتفاقيات بازل II و III، مما يساهم في تقليل المخاطر المالية والقانونية.

3.1. من منظور استراتيجي: (Nguyen & Järv, 2019):.

خارطة المخاطر التشغيلية أداة تُستخدم لتحديد وتحليل المخاطر المحتملة في العمليات المصرفية، مما يمكن المؤسسات المالية من اتخاذ قرارات استراتيجية مستندة إلى بيانات دقيقة حول المخاطر المحتملة.

4.1. من منظور المخاطر الخارجية: (Zhang & Wang, 2019):.

خارطة المخاطر التشغيلية توفر تصورًا واضحًا للمخاطر الناتجة عن العوامل الخارجية، مثل التقلبات الاقتصادية، وعدم استقرار الأسواق المالية، والكوارث الطبيعية، مما يساعد المؤسسات على تعزيز قدرتها على التكيف مع الأزمات .

5.1. من منظور الحوكمة: (Bessis, 2015):.

تساعد خارطة المخاطر التشغيلية المؤسسات المالية على تحسين الحوكمة من خلال تحديد المسؤوليات الإدارية المتعلقة بإدارة المخاطر مما يساهم في تعزيز الرقابة الداخلية وتقليل احتمالية وقوع الأخطاء التشغيلية.

6.1. من منظور العلاقة بين المخاطر والعوائد: (Osei & Asevorane, 2020):.

خارطة المخاطر التشغيلية هي وسيلة تحليلية تساعد المؤسسات المالية على تحقيق التوازن بين المخاطر والعوائد من خلال توفير رؤية شاملة حول المخاطر التشغيلية وتأثيرها على الأداء المالي.

2. الأهمية والأهداف من إعداد خارطة المخاطر البنكية:

تُعد خارطة المخاطر البنكية أداة استراتيجية وفعالة تعتمد على المؤسسات المالية من أجل تحديد وتحليل وتقييم مختلف أنواع المخاطر التي قد تواجهها.

إعداد هذه الخارطة لا يقتصر فقط على رصد النقاط الحساسة داخل البنك، بل يتجاوز ذلك ليشكل إطاراً مرجعياً لاتخاذ قرارات مبنية على أسس علمية وواقعية في هذا السياق، يبرز الجدول رقم 3 لتوضيح الأهمية البالغة التي تكتسبها خارطة المخاطر البنكية، بالإضافة إلى الأهداف الرئيسية التي تسعى المؤسسة إلى تحقيقها من خلال إعدادها واعتمادها ضمن منظومتها العامة لإدارة وتسيير المخاطر.

الجدول رقم 3: الأهمية والأهداف من إعداد خارطة المخاطر البنكية

المصدر	الأهمية	المصدر	أهداف
Bessis, 2015	تمكين الإدارة من اتخاذ قرارات مستنيرة حول المخاطر المحتملة	Onyiriuba, 2016	تحديد المخاطر المحتملة التي قد تؤثر على العمليات المصرفية.
Basel Committee, 2011	يساعد على تقليل التكاليف الناتجة عن المخاطر التشغيلية.	Girling,) (2013	تحليل مدى تأثير المخاطر المختلفة على أداء البنك
Agarwal & Dhar, 2014	الامتثال للوائح المصرفية المحلية والدولية	Basel Committee 2011	التأكد من توافق العمليات المصرفية مع المعايير الدولية مثل بازل III
Mebarki & Benali, 2022	رفع مستوى الشفافية والمصادقية في البنك	Bellini,) (2016	تطوير أنظمة رقابة داخلية قوية للحد من الأخطاء التشغيلية

تابع للجدول أعلاه ص 56.

(Loader, 2006)	تحسين عمليات البنك وتقليل الهدر في الموارد.	Gregoriou2009	إعداد خطط طوارئ لمواجهة المخاطر غير المتوقعة
Arora & Rahman, 2018	تقليل المخاطر التي قد تؤثر على سمعة البنك	Zhang & Wang, 2019	تحسين الأداء المالي عبر إدارة المخاطر بفعالية
Bouras & Khelifi, 2019	تطوير آليات أفضل لمراقبة العمليات المصرفية	Nguyen & Jara, 2019	توفير رؤية شاملة للمخاطر عبر جميع الأقسام.
Zouari & Bouzid, 2021	ضمان استمرارية البنك في بيئة مالية متغيرة.	Akhter & Hossain, 2020	تقليل المخاطر المرتبطة بالمنتجات المالية الجديدة
Osei & Asevorwese, 2020	تقليل التعرض للمخاطر السيبرانية الحد من الهجمات الإلكترونية وتأمين البيانات	Mebarki & Benali, 2022	نشر ثقافة الوعي بالمخاطر بين الموظفين
Akinwumi & Ojo, 2018	دعم النمو المستدام: تسهيل توسع البنك في الأسواق الجديدة بأمان	Cheongbai, Jojoa & Yu, 2010	مساعدة البنك على التميز عبر إدارة مخاطر أكثر كفاءة.

المصدر: من إعداد الطلب

المطلب الثاني: خصائصها وتصنيفاتها في القطاع البنكي

1. الخصائص الأساسية للمخاطر التشغيلية:

تُعد المخاطر التشغيلية من أبرز التحديات التي تواجه البنوك، نظرًا لارتباطها بالأنظمة والعمليات الداخلية والأخطاء البشرية. ويهدف هذا الجزء إلى إبراز الخصائص الأساسية لهذه المخاطر لفهم طبيعتها وتمييزها عن باقي أنواع المخاطر، مما يسهم في تحسين طرق إدارتها والتقليل من تأثيرها.

1.1. صعوبة التحديد:

تُعد المخاطر التشغيلية معقدة من حيث التحديد نظرًا لتعدد مصادرها وتتنوع تأثيراتها داخل البنك. فهي لا تقتصر على فشل الأنظمة، بل تشمل أيضًا المخاطر المرتبطة بالسلوك البشري، مثل الاحتيال والأخطاء المتعمد والغير المتعمد وهذه الأخيرة تنقسم إلى طبيعة سلوكية أو صفات شخصية في الانسان.

2.1. صعوبة القياس:

على عكس المخاطر المالية التي يمكن قياسها بوضوح من خلال المعاملات المالية، فإن المخاطر التشغيلية يصعب قياسها بدقة. فبعض التأثيرات، مثل الخسائر المالية المباشرة الناتجة عن الاحتيال، يمكن تقديرها، بينما يصعب قياس تأثيرات أخرى، مثل الأضرار التي تلحق بسمعة البنك (Lamarque & Maurer, 2009).

3.1. تحديات المراقبة والتحكم:

تتميز المخاطر التشغيلية بطبيعة متغيرة، مما يجعل من الصعب وضع أنظمة رقابية شاملة تتحكم بها بشكل كامل. يتطلب الحد من هذه المخاطر اعتماد أنظمة إدارة مخاطر متطورة، وتحديث مستمر لآليات الحوكمة والرقابة الداخلية (BCBS, 2011).

4.1. ارتباطها بالمخاطر الأخرى:

تتداخل المخاطر التشغيلية مع أنواع أخرى من المخاطر مثل مخاطر السوق والائتمان. على سبيل المثال، قد يؤدي خلل في النظام الداخلي إلى سوء تقييم العملاء، مما يزيد من مخاطر الائتمان. كذلك، قد تؤدي مشكلات الامتثال التنظيمي إلى تداعيات قانونية تؤثر على استقرار البنك (Nelson & Winter, 1982).

2. تصنيف المخاطر التشغيلية:

قدّمت لجنة بازل للرقابة المصرفية تصنيفاً يشمل سبعة أنواع رئيسية من المخاطر، يُعرف بـ"عائلة بازل السبعة" بهدف تعزيز إدارة المخاطر وتوحيد المفاهيم في القطاع المصرفي لضمان الاستقرار المالي وهي كالتالي:

1.2. الاحتيال الداخلي:

مخاطر ناتجة عن أفعال احتيالية يرتكبها موظفو المؤسسة عمدًا، كإساءة استخدام المنصب أو تزوير مستندات لتحقيق منفعة شخصية.

أمثلة:

- موظف يزور توقيع عميل لسحب أموال.
- تحويل غير مصرح به لحساب خاص.
- سرقة ممتلكات البنك.

2.2. الاحتيال الخارجي:

مخاطر ناتجة عن أطراف خارجية تستهدف المؤسسة بوسائل احتيالية، مثل الهجمات الإلكترونية أو التزوير.

أمثلة:

- متسلل يسرق بيانات بطاقات العملاء.
- شخص ينتحل هوية عميل لسحب الأموال.
- تزوير شيكات أو بطاقات ائتمان.

3.2. علاقات العمل وسلامة الموظفين:

مرتبطة بالنزاعات بين الموظفين والإدارة أو ظروف العمل غير الآمنة.

أمثلة:

- موظف يقاضي المؤسسة بسبب بيئة غير صحية.
- حادث شغل ناتج عن إهمال في إجراءات السلامة.
- دعوى بسبب تمييز أو تحرش.

4.2. العملاء، المنتجات، والممارسات التجارية:

تنشأ من سوء تقديم المنتجات أو خرق الالتزامات تجاه العملاء.

أمثلة:

- بيع منتج مالي دون شرح مخاطره.
- خرق شروط عقد مع عميل.
- فرض رسوم غير مبررة.

5.2. الأضرار المادية للأصول:

خسائر بسبب حوادث طبيعية أو بشرية تلحق ضرراً بالأصول المادية البنك.

أمثلة:

- زلزال يدمر فرع بنكي.
- حريق في مقر البنك.
- أعمال تخريب خلال مظاهرات.

6.2. تعطل الأنشطة والأنظمة:

مخاطر ناتجة عن توقف العمل بسبب خلل تقني أو بنية تحتية.

أمثلة:

- توقف النظام البنكي فجأة.
- انقطاع الكهرباء عن مركز البيانات.
- فشل في نظام المعالجة الآلية.

7.2. الأخطاء في تنفيذ العمليات:

أخطاء في المعاملات اليومية أو ضعف الرقابة الداخلية.

أمثلة:

- تحويل مالي إلى حساب خاطئ.
- إدخال بيانات غير صحيحة.

- فقدان ملفات أو مستندات هامة.

المطلب الثالث: أدوات ومنهجية إعداد الخارطة

1. منهجية إعداد خارطة المخاطر البنكية:

تعتمد خارطة المخاطر البنكية على منهجية منظمة تهدف إلى تحديد وتقييم وتصنيف المخاطر حسب درجة خطورتها. يستعرض هذا الجزء خطوات إعداد هذه الخارطة لضمان فهم شامل للمخاطر التي قد تواجه البنك.

1.1. تحديد نطاق التحليل:

يتم في هذه المرحلة تحديد العمليات المصرفية الأساسية التي ستخضع للتحليل، مثل القرض، التحويلات المالية، وإدارة الأصول. كما يتم تحديد المسؤوليات لكل قسم لضمان شمولية التحليل (Ghanmi, 2014)

2.1. جمع البيانات وتحديد مصادر المخاطر:

تشمل هذه الخطوة جمع البيانات من تقارير الحوادث، مراجعة التدقيق الداخلي، واستطلاعات الموظفين. يتم تصنيف مصادر المخاطر إلى داخلية (مثل الأخطاء البشرية والاحتيال الداخلي) وخارجية (مثل التغيرات التنظيمية والكوارث الطبيعية) (Renard, 2017).

3.1. تقييم وتصنيف المخاطر:

يتم استخدام منهجيات مثل:

- التقييم الذاتي المخاطر وأنظمة الرقابة ((Risk and Control Self Assessment)

- طريقة بطاقات التقييم "Scorecard" لتحديد المخاطر الأكثر تأثيرًا.

- تحليل السيناريوهات لتقييم المخاطر المحتملة.

تقديم شرح موجز للطرق الثلاثة:

1. طريقة RCSA: يمكن تطبيقها وفق لثلاثة مراحل رئيسية وهي:

أولاً: تحديد نطاق التطبيق:

في هذه المرحلة، تقرر المؤسسة ما إذا كانت ستطبق RCSA على جميع المخاطر التشغيلية أو فقط على فئات محددة (مثل المخاطر ذات التأثير الكبير أو المتعلقة بأهداف استراتيجية أو عمليات حرجة). يمكن اعتماد نهج شامل أو جزئي حسب الموارد المتاحة.

الهدف: التركيز على أكثر المخاطر تأثيراً وتفادي الإرهاق الإداري. (IOR, 2021)

ثانياً: تحديد المنهجية:

يتم الاختيار بين منهجين رئيسيين:

– **المنهج القائم على الحدث (Event-Based):** يركز على أحداث محددة مثل: الاحتيال، فشل النظام، الكوارث.

– **المنهج القائم على العملية (Process-Based):** يركز على سير العمليات وتحديد نقاط الفشل المحتملة فيها.

الاختيار يعتمد على مدى توفر خرائط العمليات وتعقيد البنية التشغيلية. (IOR, 2021)

ثالثاً : توزيع الأدوار والمسؤوليات:

يتم تحديد الجهات المسؤولة عن تنفيذ RCSA، وتشمل:

– **الهيئة الإدارية:** تضمن وجود نظام تحكم فعال.

– **مالكوا المخاطر (Risk Owners):** يقيّمون ويتابعون المخاطر والضوابط.

- الإدارة العليا: تدعم تنفيذ RCSA وتراقب النتائج.

- المدقق الداخلي: يراجع فعالية العملية.

التعاون بين جميع الأطراف ضروري لضمان التقييم الواقعي. (IOR, 2021)

رابعاً : تحديد التواتر والتوقيت: (IOR, 2021,)

يتم تحديد متى وكما مرة سيتم إجراء RCSA (عادةً سنويًا).

لكن يمكن تنفيذ مراجعات غير دورية إذا ظهرت مخاطر جديدة أو تغيرت بيئة العمل.

من الأفضل إجراء RCSA قبل مراجعات الأداء السنوية لتضمين النتائج في التخطيط.

خامساً: تصميم نموذج (RCSA Template Design):

يتم إعداد نموذج تقييم يحتوي على عناصر مثل:

- تقييم المخاطر الكامنة (الخامة)

- قياس فعالية الضوابط وأنظمة المراقبة

- تقييم المخاطر الصافية (المتبقية)

- أسباب وآثار المخاطر

- إعداد خطط العمل

النموذج يمكن أن يكون ملف Excel أو نظام معلوماتي مخصص. (IOR, 2021)

سادساً: جمع البيانات:

يتم جمع المعلومات باستخدام:

- ورش عمل جماعية: تتيح النقاش المباشر وتقليل التحيز.

- استبيانات: أكثر مرونة، خاصة للموظفين البعيدين.

- طرق بديلة: مثل تحليل الأسباب الجذرية (Root Cause Analysis)

أو تقنية دلفي (Delphi).

الدمج بين الطرق يعطي نتائج أكثر دقة وواقعية. (IOR, 2021)

سابعاً :دمج النتائج في إطار إدارة المخاطر:

بعد جمع وتحليل البيانات، يتم:

- ربط النتائج ببيانات الخسائر الداخلية والخارجية.

- إعداد تقارير للإدارة العليا.

تصميم خطط تصحيحية SMART (محددة، قابلة للقياس، واقعية).

تساعد هذه الخطوة على تحسين الاستجابة للمخاطر وتعزيز الحوكمة. (IOR, 2021)

2. طريقة Scorecard:

تُعتبر طريقة Scorecard من الأدوات الكمية المستخدمة في تقييم المخاطر التشغيلية، حيث تعتمد

على جمع بيانات نوعية وكمية حول الأحداث المحتملة وتصنيفها ضمن بطاقات تقييم. تساهم هذه

الطريقة في قياس مستوى المخاطر بطريقة منظمة تساعد في اتخاذ قرارات دقيقة بشأن سبل الحد منها

وهي تمر بسبعة مراحل رئيسية:

أولاً: تحديد الأهداف ونطاق التطبيق: (Basel II Sound Practices, 2003)

في البداية، يتم تحديد الغرض من استخدام بطاقة القياس: هل هي لرصد المخاطر التشغيلية؟ أم

للمخاطر الائتمانية؟ أم لجميع أنواع المخاطر؟

كما يُحدد النطاق (مثل قسم معين أو المؤسسة بأكملها).

وضوح الهدف يُساعد في تصميم المؤشرات وتحديد البيانات المطلوبة.

ثانياً :. اختيار وتصميم المؤشرات:

يتم تحديد المؤشرات الرئيسية التي تُستخدم لتقييم المخاطر، وهي تنقسم عادة إلى نوعين:

- مؤشرات كمية (Quantitative) مثل: عدد الخسائر، القيمة المالية، وتكرار الحوادث.

- مؤشرات كيفية (Qualitative) مثل: فعالية الضوابط، الالتزام بالقوانين، درجة وعي

الموظفين.

كل مؤشر يُعطى وزناً (Weight) حسب أهميته، مما يسمح بتجميع النقاط بطريقة موضوعية.

(COSO ERM Framework, 2017)

ثالثاً : إعداد مقياس النقاط: (IRM Guide to Risk Scorecards, 2020)

تُحدّد الدرجات لكل مؤشر ضمن مقياس معين (مثلاً من 1 إلى 5 أو من 1 إلى 10)، مع تعريف

واضح لكل درجة.

مثال:

- 1-2 = خطر منخفض

- 3-4 = خطر متوسط

- 5 = خطر مرتفع

المقياس يجب أن يكون بسيطاً، واضحاً، وسهل التفسير من قبل المستخدمين.

رابعاً : جمع البيانات:

يتم جمع البيانات من مصادر مختلفة: أنظمة المعلومات، التقارير التشغيلية، نتائج التدقيق، استبيانات

الموظفين، وغيرها.

دقة البيانات مهمة لضمان صحة النتائج النهائية. (ISO 31000:2018)

خامسا : حساب النتائج وتجميع النقاط:

لكل وحدة أو نوع خطر، تُجمع الدرجات الناتجة عن المؤشرات المختلفة، ويتم احتساب المجموع الكلي أو المتوسط المرجح.

يمكن استخدام جداول أو لوحات تحكم (Dashboards) لتقديم النتائج بطريقة بصرية (مثل:

Heatmaps، الخريطة الحرارية. (KPMG Risk Scorecard Framework, 2019)

سادسا: التحليل واتخاذ القرار: (IRM, 2021; COSO, 2017)

يُستخدم مجموع النقاط لتحديد ما إذا كانت المخاطر مقبولة أو تستدعي تدخل.

- إذا كانت النتيجة مرتفعة → تُقترح إجراءات تصحيحية.

- إذا كانت ضمن المقبول → تُستمر الضوابط الحالية.

يُستخدم هذا التقييم أيضًا في التخطيط الاستراتيجي وإعداد تقارير المخاطر للإدارة العليا.

سابعاً : التحديث والمراجعة الدورية:

يجب تحديث بطاقة القياس بشكل دوري (ربع سنوي أو نصف سنوي)، خاصةً عند ظهور مخاطر

جديدة أو تغير في البيانات التشغيلية.

المراجعة المنتظمة تضمن ملاءمة الأداة ودقتها عبر الزمن. (BCBS, 2011)

3. طريقة تحليل السيناريوهات لتقييم المخاطر المحتملة:

تُعد طريقة تحليل السيناريوهات من الأساليب الفعالة في تقييم المخاطر المحتملة، حيث تعتمد على

تصور مجموعة من الحالات المستقبلية المحتملة وما قد يترتب عنها من تأثيرات. تساعد هذه المنهجية

في استباق الأحداث وتقدير درجة الخطورة، مما يُمكن المؤسسات البنكية من وضع خطط استجابة أكثر دقة وفعالية.

أولاً: تحديد الهدف والنطاق:

يتم تحديد الغرض من تحليل السيناريو: هل هو لتقييم المخاطر التشغيلية؟ أم لتقدير رأس المال المطلوب لمخاطر معينة؟ كما يُحدّد النطاق (مثل قسم تكنولوجيا المعلومات أو العمليات اللوجستية).
وضوح النطاق يُسهم في صياغة سيناريوهات دقيقة ومفيدة. (BCBS, 2011)

ثانياً : تحديد المخاطر الحرجة:

يُركّز التحليل على المخاطر ذات التأثير الكبير، والتي يصعب تقييمها من خلال البيانات التاريخية فقط، مثل الهجمات الإلكترونية، الكوارث الطبيعية، أو الاحتيال واسع النطاق.
هذه المخاطر تُسمّى "Tail Risks" أي المخاطر القصوى النادرة. (BCBS, 2011)

ثالثاً : تطوير سيناريوهات مفترضة: (BCBS, 2011; IOR, 2021)

يتم إنشاء سيناريوهات مفترضة تمثل تطورات واقعية أو ممكنة للمخاطر. كل سيناريو يتضمن:

– الحدث المحفّز (Trigger event)

– تسلسل التأثيرات

– الأطراف المتأثرة

ينبغي أن تكون السيناريوهات واقعية لكنها صادمة بما يكفي لاختبار حدود المؤسسة.

رابعاً : تقدير التأثير والاحتمالية: (BCBS, 2011; IOR, 2021)

لكل سيناريو، يتم تقدير:

– الاحتمالية (Likelihood): كم مرة قد يحدث السيناريو خلال فترة معينة.

– التأثير (Impact): مالي، تشغيلي، قانوني، أو تأثير على السمعة.

تُستخدم مقاييس كمية أو نوعية مثل الجداول الاحتمالية أو مصفوفات

(RAM- Risk .Assessment Matrix)

خامسا : إعداد مصفوفة تصنيف وتقييم المخاطر (RAM) من خلال التكرار وشدة التأثير: تُستخدم

مصفوفة تصنيف وتقييم المخاطر كأداة فعالة لتحديد درجة خطورة كل نوع من المخاطر، وذلك من

خلال الجمع بين تكرار حدوثها وشدة تأثيرها. تساهم هذه الأداة في تسهيل عملية اتخاذ القرار وتحديد

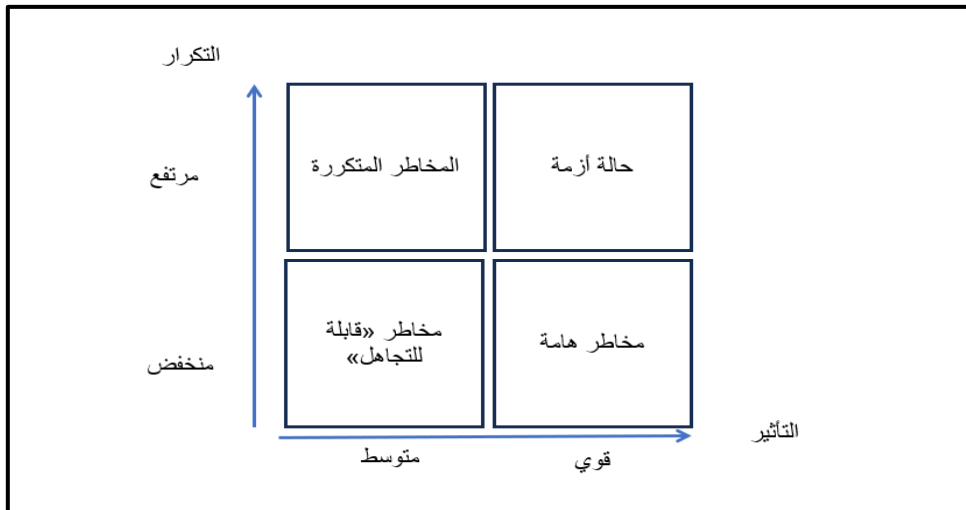
الأولويات في التعامل مع المخاطر التشغيلية

الشكل 6 يوضح مصفوفة تصنيف وتقييم المخاطر بناءً على تكرار حدوثها وشدة تأثيرها. تساعد هذه

المصفوفة في تحديد مستوى الخطورة لكل نوع من المخاطر التشغيلية، مما يسهل اتخاذ الإجراءات

المناسبة للحد منه

الشكل 6: مصفوفة تصنيف وتقييم المخاطر من خلال التكرار وشدة التأثير



Ferrary, M. (2009). Les ressources humaines à risque dans le secteur : المصدر

bancaire : Une application de la gestion des risques opérationnels. Gestion

2000, 26, 75–90 P86

سادسا : إشراك أصحاب الخبرة: (IOR, 2021; COSO, 2017)

يُستفاد من خبراء في المجالات المعنية (مثل الأمن السيبراني، العمليات المالية، الشؤون القانونية) لصياغة وتدقيق السيناريوهات.

طريقة Delphi أو ورشات العمل تُستخدم لتقليل التحيز وتعزيز الواقعية.

سابعا : مراجعة الضوابط وخطط الاستجابة:

بعد تحليل السيناريوهات، يتم تقييم مدى كفاية الضوابط الحالية، وتحديد الإجراءات المطلوبة للحد من التأثيرات المحتملة أو تحسين الجاهزية.

الهدف هو تقليل الفجوة بين الواقع والمخاطر المستقبلية المفترضة. (BCBS, 2011)

ثامنا : دمج النتائج في تقارير المخاطر:

يتم تضمين نتائج تحليل السيناريوهات في تقارير الحوكمة، واتخاذ القرار بشأن تخصيص الموارد، أو إعداد خطط استجابة واحتياطات مالية.

يدعم هذا التحليل إدارة الأزمات والتخطيط الاستراتيجي. (BCBS, 2011)

1.4. تصميم خارطة المخاطر البنكية

يعد تصميم خارطة المخاطر البنكية خطوة أساسية في إطار إدارة المخاطر، حيث تتيح هذه الأداة تصوراً شاملاً لمختلف أنواع المخاطر التي قد تواجه النظام البنكي، بما في ذلك تلك المرتبطة ببطاقات الدفع.

ومن خلال تصنيفها حسب درجة التأثير والاحتمالية، تسهم خارطة المخاطر في تسهيل المتابعة واتخاذ

القرارات الوقائية المناسبة

تشمل هذه الخارطة:

- تمثيل بياني للمخاطر حسب شدتها واحتمالية وقوعها.

– تصنيف المخاطر حسب الفئات التشغيلية والتأثير المالي.

– تحديد التدابير الوقائية لكل نوع من المخاطر (Mareschal, 2003).

1.5. تنفيذ استراتيجيات الحد من المخاطر

يُعد تنفيذ استراتيجيات الحد من المخاطر خطوة حاسمة في إطار تعزيز أمان أنظمة الدفع البنكية. فبعد تحديد وتقييم المخاطر، تأتي مرحلة التطبيق العملي للإجراءات الوقائية والتصحيحية التي تهدف إلى تقليل احتمالية حدوث المخاطر أو التخفيف من آثارها. ويساهم هذا التنفيذ المنهجي في تحسين فعالية نظام إدارة المخاطر وتعزيز الثقة في استخدام بطاقات الدفع تتمثل في:

– تعزيز نظم الرقابة باستخدام أدوات تحليل البيانات:

تعتمد البنوك على تقنيات مثل التحليل التنبؤي وأنظمة التنبيهات المبكرة لرصد السلوكيات غير الاعتيادية واكتشاف الاحتيال أو الخلل في العمليات.

– تشمل الأنظمة: التحقق المزدوج، التحكم في الوصول، والتجزئة الوظيفية (BCBS, 2011).

– مراجعة السياسات والإجراءات لضمان الامتثال:

تشمل مراجعة الإجراءات المتعلقة بفتح الحسابات، مكافحة غسل الأموال، الأمن السيبراني، والإقراض. وتستخدم أنظمة تتبع آلية لضمان الامتثال المستمر (BCBS, 2011).

– تدريب الموظفين على المخاطر التشغيلية:

يشمل التدريب مهارات التبليغ عن الحوادث، الاستجابة للحالات الطارئة، وفهم الضوابط الداخلية، باستخدام المحاكاة أو التعلّم الإلكتروني (COSO ERM Framework, 2017).

– الاستعانة بجهات خارجية لتقليل بعض المخاطر:

يُستخدم التعاقد الخارجي في وظائف مثل الأمن السيبراني أو التدقيق، مع فرض ضوابط مثل

مراجعة الأداء وتقييم الطرف الثالث. (BCBS, 2011)

8. المتابعة والتحديث المستمر:

يتم تحديث خارطة المخاطر بشكل دوري وفقاً للمتغيرات التنظيمية والاقتصادية، مع إدخال

مؤشرات قياس جديدة (Lamarque, 2011)

المطلب الرابع: الاستخدامات الرئيسية لخريطة المخاطر في البنوك

1. الاستخدامات الرئيسية لخريطة المخاطر في البنوك:

تمثل خريطة المخاطر أداة استراتيجية شاملة تُستخدم في القطاع البنكي لتحديد وتصنيف المخاطر وفقاً لطبيعتها وتأثيرها المحتمل.

ولا تقتصر فائدتها على التقييم، بل تمتد لتشمل مجموعة من الاستخدامات العملية التي تُسهم في تعزيز فاعلية النظام الرقابي، ودعم الامتثال، وتحسين كفاءة الأداء واتخاذ القرار وفيما يلي نستعرض أهم الاستخدامات الرئيسية لخريطة المخاطر في البنوك.

1.1. مجلس الإدارة:

يستخدم مجلس الإدارة خريطة المخاطر لتوجيه استراتيجية البنك وضمان توازنها مع مستوى المخاطر المقبول. تُساعد الخريطة في مراقبة فعالية نظام إدارة المخاطر، وتحديد الأولويات الرقابية، وضمان توافق السياسات مع التحديات المستقبلية.

تنوه لجنة بازل إلى أن وجود خبراء مستقلين في إدارة المخاطر ضمن المجلس يُعزز من قدرته على

الإشراف الفعّال على المخاطر. (BCBS, 2015)

2.1. المديرية العامة:

تعتمد الإدارة التنفيذية على خريطة المخاطر لتخصيص الموارد، تطوير السياسات، وتحديد أولويات العمل. تُستخدم الخريطة لتقييم المخاطر التشغيلية والمالية، وضمان استجابة فعّالة للتغيرات في بيئة الأعمال. (OCC, 2016)

3.1. أعضاء المراقبة الداخلية:

تُعد خريطة المخاطر أداة أساسية لأعضاء المراقبة الداخلية، حيث تُستخدم لتخطيط وتنفيذ عمليات التدقيق الداخلي بناءً على تقييم المخاطر. تُساعد في تحديد المجالات ذات المخاطر العالية، وتوجيه جهود التدقيق نحوها، مما يُعزز من فعالية الرقابة الداخلية. (European Central Bank, 2024)

4.1. هيئات الرقابة الخارجية:

تستخدم هيئات الرقابة الخارجية خريطة المخاطر لتقييم مدى فعالية نظام إدارة المخاطر في البنك. تُساعد الخريطة في تحديد المجالات التي تحتاج إلى مراجعة دقيقة، وضمان التزام البنك بالمعايير التنظيمية. (BCBS, 2015)

5.1. المديریات:

تُستخدم خريطة المخاطر على مستوى الفروع والمديريات المركزية لتحديد المخاطر المحلية، مثل المخاطر التشغيلية أو الامتثال التنظيمي. تُساعد في تطوير خطط استجابة مخصصة، وضمان تماشي العمليات مع السياسات العامة للبنك (BCBS, 2011)

2. الفرق بين خريطة المخاطر التشغيلية وخريطة المخاطر الأخرى

تُعد خريطة المخاطر التشغيلية إحدى الأدوات الأساسية في إدارة المخاطر المصرفية إلا أنها تختلف عن الخرائط الأخرى مثل خريطة المخاطر الائتمانية وخريطة المخاطر السوقية من حيث طبيعة المخاطر التي تُعالجها وأساليب تحليلها وإدارتها. (Hull, 2010)

3. الاعتبارات التنظيمية في إعداد خريطة المخاطر:

تُعد الاعتبارات التنظيمية عنصرًا محوريًا في إعداد خريطة المخاطر، حيث تسهم في ضمان التزام المؤسسات بالضوابط الرقابية والمعايير المعتمدة من الجهات التنظيمية، مما يعزز فعالية إدارة المخاطر ويدعم الامتثال والشفافية.

4. أدوات وتقنيات إعداد خريطة المخاطر التشغيلية

إعداد خريطة المخاطر التشغيلية يتطلب استخدام مجموعة متنوعة من الأدوات والتقنيات التي تساعد المؤسسات المالية على تحديد وتحليل وإدارة المخاطر التشغيلية يشمل ذلك دمج التكنولوجيا المتقدمة وتحليل البيانات الضخمة، وتطبيق النماذج الكمية وتقنيات الذكاء الاصطناعي بهدف تحسين دقة التقييم والاستجابة الفعالة للمخاطر المحتملة.

5. دور التكنولوجيا في إعداد خريطة المخاطر التشغيلية

في العصر الرقمي أصبحت التكنولوجيا أداة أساسية في تحسين دقة وكفاءة إدارة المخاطر التشغيلية تساعد الأدوات التكنولوجية على جمع وتحليل كميات هائلة من البيانات بسرعة ودقة مما يسهل التعرف على الأنماط والتنبؤ بالمخاطر المستقبلية وتشمل هذه الأدوات:

1.5. الذكاء الاصطناعي والتعلم الآلي: وفقاً لـ **Agarwal & Dhair (2014)**، يساهم الذكاء

الاصطناعي في تعزيز القدرة على اكتشاف الأنماط الخفية داخل البيانات مما يساعد المؤسسات المالية في التنبؤ بالمخاطر التشغيلية واتخاذ قرارات استباقية للحد منها.

2.5. البلوك تشين والأمان السيبراني: أشارت دراسة **Chernobai, Jorion, & Yu (2010)** إلى

أن تقنية البلوك تشين تساهم في تعزيز الشفافية وتقليل الاحتيال المالي من خلال توفير سجل غير قابل للتغيير لجميع العمليات المالية، مما يقلل من المخاطر التشغيلية المرتبطة بالاحتيال والاحتيال الإلكتروني.

3.5. التحليلات التنبؤية والتعلم الآلي: تلعب التحليلات المتقدمة والتعلم الآلي دوراً متزايداً في التنبؤ

بالمخاطر التشغيلية. وفقاً لـ **Nguyen & Jean (2019)** تعتمد البنوك بشكل متزايد على الذكاء الاصطناعي لتحديد العوامل المؤدية إلى المخاطر التشغيلية قبل حدوثها مما يُمكنها من اتخاذ تدابير استباقية لحماية عملياتها.

4.5. استخدام البيانات الضخمة في تحليل المخاطر التشغيلية:

يُعد تحليل البيانات الضخمة (Big Data Analytics) من الأدوات المهمة في إعداد خريطة المخاطر التشغيلية إذ يُمكن المؤسسات من استخدام تقنيات تحليلية متقدمة لاستخلاص رؤى أعمق حول أنماط المخاطر.

5.5. تحليل بيانات الحوادث السابقة:

يجمع هذا النهج البيانات المتعلقة بالحوادث التشغيلية السابقة لتحليل الأنماط المتكررة للأخطاء التشغيلية والعمل على تجنبها مستقبلاً (Bessis, 2015).

6.5. استخدام التعلم الآلي لتحليل المخاطر: وفقاً لـ **Nguyen & Jean (2019)** يمكن خوارزميات التعلم العميق من التعرف على الأنماط الشاذة في العمليات المصرفية مما يسهم في الكشف المبكر عن التهديدات وتقليل معدلات الاحتيال.

7.5. تحليل السيناريوهات: تُستخدم النماذج الإحصائية والتعلم الآلي لمحاكاة سيناريوهات المخاطر المحتملة وتوقع تأثيراتها على العمليات المختلفة داخل المؤسسة المالية مما يساعد في تطوير استراتيجيات وقائية أكثر كفاءة (Bessis, 2015).

8.5. توظيف البلوك تشين لتعزيز الأمن السيبراني: حسب **Chernobai, Jorion & Yu (2010)** فإن استخدام تقنيات البلوك تشين يسهم في تأمين البيانات وتحقيق الشفافية في العمليات المصرفية مما يقلل من احتمالية التعرض للاحتيال.

9.5. إدارة المخاطر التشغيلية من خلال التقنيات السحابية: تعد الحوسبة السحابية حلاً فعالاً لتخزين وتحليل البيانات بشكل سريع وفعال حيث تتيح إمكانية الوصول إلى البيانات من أي مكان وفي أي وقت مما يعزز من مرونة المؤسسات المالية في التعامل مع المخاطر الناشئة (BCBS, 2011).

6. تطبيقات خريطة المخاطر التشغيلية في مختلف القطاعات المصرفية

تُستخدم خريطة المخاطر التشغيلية كأداة فعالة لتحديد المخاطر وتحليلها والتخفيف من أثارها في القطاع المصرفي وفيما يلي تطبيقاتها في مجالي إدارة عمليات الدفع والتحويلات المالية والامتثال ومكافحة الجرائم المالية.

1.6. تطبيق خريطة المخاطر التشغيلية في إدارة عمليات الدفع والتحويلات المالية:

تواجه عمليات الدفع والتحويلات المالية العديد من المخاطر التشغيلية، مثل فشل الأنظمة والأخطاء البشرية والهجمات السيبرانية والامتثال غير الكافي للوائح.

2.6. تحسين أمان أنظمة الدفع: أشارت دراسة Mishra & Gupta (2022) إلى أن تحليل المخاطر التشغيلية يساعد في تحديد نقاط الضعف في أنظمة الدفع مما يؤدي إلى تعزيز الأمن السيبراني والحد من الاحتيال المالي.

3.6. التكيف مع التكنولوجيا الحديثة: أظهرت دراسة Kumar & Singh (2020) أن التطورات التكنولوجية عززت كشف الاحتيال لكنها في الوقت ذاته فرضت تحديات جديدة مما يستدعي تحديث خرائط المخاطر التشغيلية بانتظام.

4.6. إدارة مخاطر المعاملات الرقمية: وفقاً لـ Zhang & Wang (2019)، فإن أنماط سلوك المستخدمين تؤثر على المخاطر التشغيلية في المدفوعات الرقمية، ما يستدعي تطوير نماذج تقييم مخاطر متكيفة مع السلوكيات المتغيرة.

5.6. التحكم في المخاطر النظامية: تناولت لجنة Basel Committee (2011) أهمية تطوير آليات صارمة لجمع البيانات حول المخاطر التشغيلية وتحليلها بشكل استباقي لتجنب التعطل في أنظمة الدفع.

6.6. تطبيق خريطة المخاطر التشغيلية في الامتثال ومكافحة الجرائم المالية:

تمثل الجرائم المالية مثل غسل الأموال وتمويل الإرهاب تحديات كبيرة تتطلب تطبيق استراتيجيات فعالة لإدارة المخاطر التشغيلية.

7.6. تحليل عمليات غسل الأموال: وجدت دراسة Arora & Rahman (2018) أن عدم الامتثال الفعال للمتطلبات التنظيمية يزيد من مخاطر غسل الأموال مما يستلزم استخدام خرائط المخاطر التشغيلية لتعزيز الامتثال. تقليل الثغرات في الامتثال: وفقاً لدراسة Akiowunri & Ojo (2018)، فإن البنوك الإفريقية تحتاج إلى تكامل أفضل لأنظمة الامتثال مع إدارة المخاطر التشغيلية، خاصة فيما يتعلق بتحديد الأنشطة المشبوهة.

8.6. تحسين إجراءات مراقبة الامتثال: أظهرت دراسة Nguyen & Tran (2019) أن الامتثال الفعال للمخاطر التشغيلية يعزز ثقة العملاء، لكنه يتطلب تحديثات مستمرة وفقاً لتغيرات اللوائح الدولية.

9.6. استخدام التكنولوجيا في مكافحة الجرائم المالية: أكدت دراسة Agarwal & Dhar (2014) أن التطورات الحديثة، مثل الذكاء الاصطناعي، يمكن أن تدعم إدارة المخاطر التشغيلية من خلال كشف التهديدات الجديدة مثل الهجمات الإلكترونية المرتبطة بالجريمة المالية

7. تقييم فعالية خريطة المخاطر التشغيلية:

تعد خريطة المخاطر التشغيلية من الأدوات الأساسية التي تساعد المؤسسات المالية على تحديد المخاطر المحتملة وتحليلها وإدارتها بفعالية ومع ذلك، لضمان كفاءتها في الحد من المخاطر التشغيلية وتعزيز الامتثال، يجب تقييم أدائها باستخدام معايير واضحة ومحددة.

8. معايير قياس كفاءة خريطة المخاطر:

لقياس فعالية خريطة المخاطر التشغيلية، يمكن استخدام المعايير التالية:

1.8. تغطية المخاطر التشغيلية: كما أشار Basel Committee (2011)، فإن خريطة المخاطر الفعالة يجب أن تغطي جميع مصادر المخاطر التشغيلية، بما في ذلك المخاطر الداخلية مثل الأخطاء البشرية والتلاعب، بالإضافة إلى المخاطر الخارجية مثل الهجمات السيبرانية والاحتيال.

2.8. مدى دقة التوقعات والتنبؤ بالمخاطر: وفقاً لدراسة Kumar & Singh (2020)، فإن خريطة المخاطر التشغيلية الفعالة هي التي توفر رؤية دقيقة للمخاطر المستقبلية المحتملة وتمكن البنوك من اتخاذ تدابير استباقية لمواجهتها.

3.8. مرونة التكيف مع التغييرات التنظيمية والتكنولوجية: يشير Agarwal & Dhar (2014)

إلى أهمية تحديث خريطة المخاطر بشكل دوري لضمان مواكبة التطورات التكنولوجية واللوائح الجديدة، خاصة في ظل تزايد الهجمات الإلكترونية.

4.8. تقييم الالتزام بلوائح الامتثال: أشارت دراسة Mebarki & Benali (2020) إلى أن فعالية

خريطة المخاطر التشغيلية تُقاس بقدرتها على مساعدة المؤسسات المالية في الامتثال للمعايير الدولية، مثل مكافحة غسل الأموال وتمويل الإرهاب.

5.8. التصدي للتهديدات السيبرانية: وفقاً لـ Osei & Asensane (2020)، يمكن أن تحد خريطة

المخاطر من التهديدات الإلكترونية التي تستهدف الأنظمة المصرفية من خلال التعرف المبكر على نقاط الضعف وتنفيذ تدابير استباقية لحمايتها.

6.8. تحليل فعالية استراتيجيات التخفيف من المخاطر: دراسة Akiowunri & Ojo (2018)

أكدت أن تقييم مدى نجاح التدابير المطبقة لمعالجة المخاطر التشغيلية يساعد في تحديد الثغرات وتطوير استراتيجيات جديدة لمكافحة الجرائم المالية وتحسين أنظمة الرقابة الداخلية.

باستخدام هذه المعايير، يمكن للبنوك تقييم مدى فاعلية خرائط المخاطر التشغيلية، وتحديث استراتيجياتها الأمنية والامتتالية بشكل مستمر لمواكبة تطورات البيئة المالية المتغيرة باستمرار.

9. تأثير التحول الرقمي على خريطة المخاطر التشغيلية:

يؤثر التحول الرقمي بشكل مباشر على طبيعة المخاطر التشغيلية في القطاع المصرفي، إذ أدت الرقمنة إلى زيادة الكفاءة وتقديم خدمات مالية أكثر مرونة، لكنها في المقابل زادت من التعقيدات والمخاطر، ومن بين هذه المخاطر نذكر المخاطر التالية:

1.9. المخاطر السيبرانية والاختراقات الإلكترونية: وفقاً لدراسة Agarwal & Dhar (2014)، فإن

التطورات التكنولوجية الحديثة جلبت تهديدات جديدة مثل الهجمات السيبرانية، مما يستوجب تحديث خريطة المخاطر التشغيلية لتعزيز التدابير الأمنية وكشف التهديدات السيبرانية المحتملة.

2.9. التوسع في حلول الدفع الرقمية والمخاطر المرتبطة بها: أكد Osei & Asensane (2020)

أن أنظمة الدفع الإلكترونية تحتاج إلى تدابير إضافية لحماية البيانات المالية وتقادي التهديدات السيبرانية التي ازدادت مع تطور التقنيات المالية.

3.9. تحديات الامتثال للوائح الرقمية المتغيرة: أشارت لجنة Basel Committee (2011) إلى

أهمية تحديث الأنظمة المصرفية لتلبية متطلبات الامتثال التنظيمي، خاصة مع التطورات المتسارعة في التكنولوجيا المالية وزيادة التهديدات الإلكترونية.

المبحث الرابع : بطاقات الدفع البنكية والمخاطر التشغيلية المرتبطة بها

أصبحت بطاقات الدفع البنكية من الأدوات الأساسية في العمليات المالية الحديثة لما توفره من سهولة وسرعة في تنفيذ المعاملات ومع ذلك فإن استخدامها المتزايد يرافقه مجموعة من المخاطر التشغيلية مثل الأخطاء التقنية الاحتيال والاختراقات الأمنية ومن هنا تبرز أهمية تحليل هذه المخاطر بهدف التعرف عليها بدقة والحد من تأثيرها على كفاءة وسلامة النظام المصرفي.

المطلب الأول :التعريف والأنواع والمراحل

1. تعريف بطاقات الدفع البنكية وأنواعها:

1.1. تعريف بطاقات الدفع البنكية:

بطاقات الدفع البنكية هي أدوات مالية إلكترونية تُستخدم لإجراء المعاملات المالية عبر الإنترنت أو في المتاجر الفعلية وهي تصدر من قبل البنوك والمؤسسات المالية المعتمدة تُمثل هذه البطاقات بديلاً فعالاً للنقد مما يسهل عمليات الشراء والدفع كما أنها توفر مستوى عالٍ من الأمان من خلال تقنيات التشفير والحماية (Kumar & Singh, 2020).

2.1. المؤسسات المصرفية المنتمية إلى الشبكة البنكية للنقديات المشتركة:

الشكل 7- يوضح المؤسسات المصرفية المنتمية إلى الشبكة البنكية للنقديات المشتركة هذه الشبكة تشكل جزءاً أساسياً من النظام المصرفي الحديث حيث تتيح للمؤسسات المالية تبادل المعاملات النقدية بشكل مشترك وفعال من خلال هذا الشكل، يتم تمثيل التنسيق بين البنوك المختلفة التي تشارك في هذه الشبكة مما يعزز من سلاسة العمليات المالية ويسهم في تحسين الخدمات المصرفية المقدمة للعملاء تم تصميم هذه الشبكة لتوفير بيئة آمنة وموثوقة لتبادل البيانات والمعاملات المالية بين البنوك.

الشكل 7: يوضح المؤسسات المصرفية المنتمية إلى الشبكة البنكية للنقديات المشتركة.



المصدر: SATIM. (N.d.). Société d'Automatisation des Transactions Interbancaires et de Monétique. <https://www.satim.dz/index.php/ar/cib-khdmat/cib> (consulté le 16/03/2025)

2. أنواع بطاقات الدفع البنكية:

تعتبر بطاقات الدفع البنكية من الأدوات المالية الأساسية في النظام المصرفي الحديث، حيث توفر وسيلة مريحة وآمنة لتنفيذ المعاملات المالية وفقاً للدراسات يمكن تصنيف بطاقات الدفع البنكية إلى الأنواع التالية:

1.2. بطاقات الائتمان (Credit Cards):

تتيح لحاملها الشراء والدفع لاحقاً حيث يمنح البنك حداً ائتمانياً يمكن استخدامه، ويتم تسديده لاحقاً بالكامل أو على أقساط بفوائد (Arora & Rahman, 2018).

من أمثلتها: **American Express ، Mastercard ، Visa**.

2.2. بطاقات الخصم المباشر (Debit Cards):

ترتبط مباشرةً بحساب العميل المصرفي حيث يتم الخصم الفوري للمبلغ عند إجراء أي معاملة (Zhang & Wang, 2019).

تُستخدم على نطاق واسع في عمليات السحب النقدي من أجهزة الصراف الآلي والمشتريات اليومية.

من أمثلتها: CIB & EDAHABIA

3.2. البطاقات مسبقة الدفع (Prepaid Cards):

يتم شحنها بمبلغ معين مسبقاً، ويمكن استخدامها حتى نفاد الرصيد مما يجعلها خياراً مثالياً للأشخاص غير المؤهلين للحصول على بطاقات الائتمان (Nguyen & Tran, 2019).

4.2. بطاقات الدفع الذكية (Smart Cards): (Mishra & Gupta, 2022).

تحتوي على شريحة إلكترونية متقدمة لتخزين المعلومات المالية وإجراء المعاملات بأمان أعلى وتُستخدم في بعض الأنظمة المصرفية المتطورة لتقليل مخاطر الاحتيال

5.2. البطاقات الافتراضية (Virtual Cards):

تُستخدم بشكل رئيسي في المعاملات عبر الإنترنت حيث لا توجد نسخة مادية منها مما يقلل من مخاطر الاحتيال الإلكتروني (Osei & Agyemang, 2020).

6.2. بطاقة الدفع (Carte de paiement): بطاقة الدفع هي أداة إلكترونية تصدرها مؤسسة مالية

وغالباً ما تكون بنكاً، وتُستخدم من قبل حاملها لإجراء معاملات مالية مثل شراء السلع والخدمات أو سحب الأموال من أجهزة الصراف الآلي

تتميز هذه البطاقات بتقنيات أمنية متطورة مثل الشريحة الذكية (EMV)، الشريط المغناطيسي، وخاصية الدفع اللائاسي (Contactless Payment). كما أنها تخضع لمعايير أمنية صارمة من أبرزها

معيار (PCI DSS (Payment Card Industry Data Security Standard)، الذي يُعد الإطار المرجعي لحماية بيانات حاملي البطاقات، وتخضع كذلك لتشريعات أمريكية مثل قانون حماية المستهلك المالي لعام 2010 ضمن Dodd–Frank Act، بالإضافة إلى تنظيمات مكتب الحماية المالية للمستهلك (CFPB) (Federal Reserve, 2021; PCI Security Standards Council, 2023)

3. العناصر الموجودة على الجهة الأمامية والخلفية للبطاقة البنكية:

تتضمن البطاقة البنكية مجموعة من العناصر الأساسية على الجهة الأمامية والخلفية التي تلعب دوراً مهماً في ضمان استخدامها بشكل آمن وفعال. من خلال هذه العناصر، يتم تحديد هوية صاحب البطاقة وتسهيل إجراء المعاملات المالية بكل سلاسة. تشمل هذه العناصر معلومات مثل الرقم التسلسلي للبطاقة، تاريخ انتهاء صلاحيتها، اسم صاحبها، وغيرها من التفاصيل التي تضمن أمن وموثوقية العمليات المالية.

الشكل 8: العناصر الموجودة على الجهة الأمامية والخلفية للبطاقة البنكية



المصدر: SATIM. (n.d.). Carte CIB. <https://www.satim.dz/index.php/ar/cib-khdmat/cib>

(Consulté le 16/04/2025)

4. الأبعاد المتفق عليها في إنتاج البطاقة حسب معايير ISO/IEC 7810:2003:

عند تصميم وإنتاج البطاقات البنكية، من الضروري الالتزام بمعايير دولية تضمن توحيد شكل

وحجم هذه البطاقات على المستوى العالمي. ومن بين أهم هذه المعايير، نجد المعيار ISO/IEC

7810:2003، الذي يحدد بدقة الأبعاد الفيزيائية للبطاقة البنكية.

وفقاً لهذا المعيار:

– **الطول** يجب أن يكون 85.60 ملم،

– **العرض** 53.98 ملم،

– **السُمك** 0.76 ملم.

الهدف من احترام هذه الأبعاد هو ضمان توافق البطاقة مع جميع الأجهزة الإلكترونية، مثل أجهزة الصراف الآلي والقراء الإلكترونية، مما يسهل استخدامها بشكل موحد وآمن عبر مختلف الدول والمؤسسات تُحدّد أبعاد البطاقة البنكية وفقاً لمعايير دولية دقيقة لضمان التوافق مع مختلف الأجهزة والأنظمة.

5. أهمية بطاقات الدفع البنكية:

في ظل التحول الرقمي المتسارع وتطور حاجات الأفراد والمؤسسات، أصبحت بطاقات الدفع البنكية أداة محورية في تقديم الخدمات المالية الحديثة. فهي تسهم بشكل فعّال في تسهيل العمليات المالية اليومية، وتقليل الاعتماد على النقد، ما يعزز من كفاءة النظام المالي ويواكب متطلبات الاقتصاد الرقمي. كما تُعتبر وسيلة مهمة لتعزيز الشمول المالي وتوفير الراحة والأمان في التعاملات المصرفية.

وتتمثل أهمية بطاقات الدفع البنكية في عدة جوانب رئيسية، من بينها:

– **الأمان:** توفر تقنيات التشفير والحماية ضد الاحتيال والاختراقات (Bouras & Khelifi, 2019).

– **الراحة:** تُغني عن حمل النقود وتُستخدم محلياً ودولياً (Zarif & Hossain, 2020).

– **التنظيم المالي:** تُسهل تتبع النفقات والتحكم في المصاريف (Mebarki & Benali, 2022).

وفقاً للدراسات الحديثة، شهدت بطاقات الدفع البنكية تطورات ملحوظة، مثل استخدام الذكاء الاصطناعي وتحليل البيانات لاكتشاف الاحتيال إلى جانب التوسع في استخدام تقنيات البلوك تشين لزيادة الأمان (Agarwal & Dhar, 2014).

6. مراحل عمل بطاقات الدفع البنكية:

تُعد بطاقات الدفع البنكية من أهم أدوات الدفع الإلكتروني، حيث تقوم على نظام متكامل يربط بين عدة أطراف من أجل تنفيذ المعاملة المالية بكفاءة وأمان. ويتطلب عمل هذه البطاقات سلسلة من الإجراءات التقنية والتنظيمية تبدأ من لحظة إدخال البطاقة أو بياناتها إلى حين تأكيد المعاملة المالية وتنفيذها. إن فهم مراحل عمل هذه البطاقات يُعد ضرورياً لتقييم المخاطر التشغيلية المرتبطة بها وتحسين أدائها.

وتتمثل مراحل عمل بطاقات الدفع البنكية في عدد من الخطوات المتسلسلة، من أبرزها:

1.6. إجراء المعاملات:

عند استخدام بطاقة الدفع البنكية في الشراء أو السحب النقدي تمر العملية بالمراحل التالية:

إدخال البطاقة أو استخدامها عبر تقنية NFC: يتم إدخال البطاقة في جهاز الدفع الإلكتروني

(POS) أو تمريرها عبر تقنية الدفع اللائق (Agarwal & Dhar, 2014).

– **التحقق من الرصيد:** يقوم البنك المُصدر بمراجعة رصيد الحساب المصرفي للعميل وإذا كان

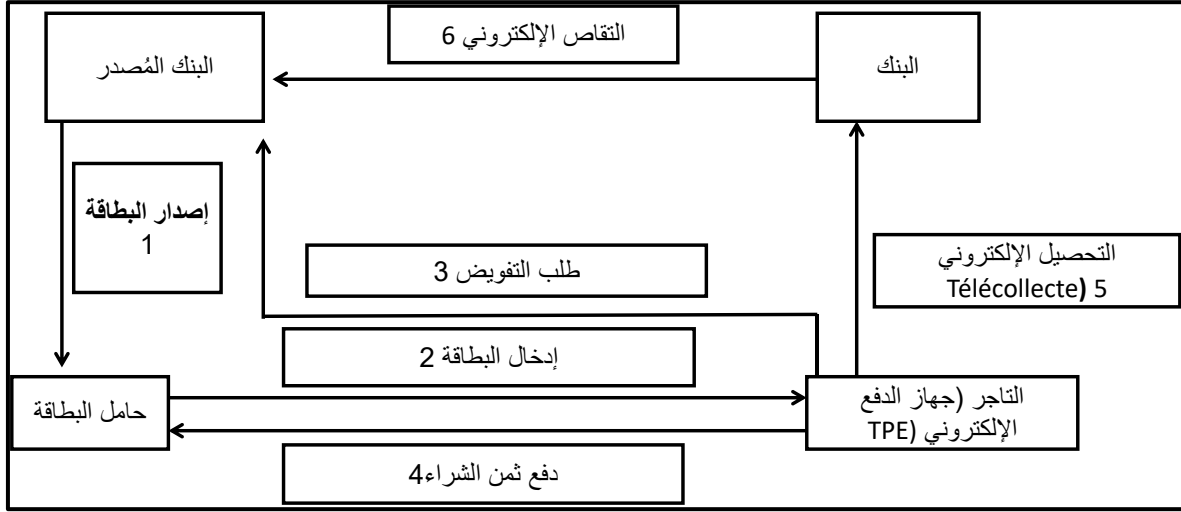
كافياً، يتم الموافقة على العملية (Nguyen & Tran, 2019).

– **تأكيد العملية وإتمام الدفع:** بعد الموافقة، يتم خصم المبلغ مباشرةً من حساب العميل وتحويله

إلى حساب التاجر خلال وقت قصير يتراوح بين بضع ثوانٍ إلى 24 ساعة (BCBS, 2011).

- التسوية المالية: تم التسوية المالية بين البنك المصدّر والتاجر من خلال شبكات الدفع مثل **Visa و Mastercard**، حيث يتم إرسال المبلغ من حساب العميل إلى حساب التاجر بعد اكتمال العملية (Osei & Agyemang, 2020).
- الأمان ومكافحة الاحتيال: نظرًا لتزايد الجرائم الإلكترونية، تعتمد بطاقات الدفع البنكية على تقنيات أمان متقدمة، منها:
 - التشفير ثنائي العامل (FA2): يتطلب إدخال رمز تحقق إضافي عند إجراء عمليات الدفع عبر الإنترنت (Mishra & Gupta, 2022).
 - أنظمة كشف الاحتيال: تستخدم الذكاء الاصطناعي لتحليل العمليات المالية واكتشاف أي نشاط مشبوه (Mebarki & Benali, 2022).
 - تقنيات الدفع اللائق والمصادقة البيومترية: مثل بصمة الإصبع أو التعرف على الوجه لتأمين العمليات (Zarif & Hossain, 2020)
- تتم عملية الدفع بواسطة البطاقة البنكية عبر جهاز الدفع الإلكتروني وفق سلسلة من الخطوات المتتابعة تهدف إلى ضمان أمان وسرعة المعاملة يعرض هذا الشكل المراحل الأساسية التي تمر بها عملية الدفع، من إدخال البطاقة وحتى الحصول على الموافقة النهائية من البنك.

الشكل 9: مراحل عمل بطاقة الدفع في جهاز الدفع الإلكتروني (TPE)



من إعدادنا باستعان بالمصادر التالية: Agarwal & Dhar, 2014؛ Nguyen & Tran, 2019؛ Osei ، 2011؛ Zarif & Hossain، ؛Mebarki & Benali, 2022؛ Mishra & Gupta, 2022؛ & Agyemang, 2020 (2020).

7. مراحل عمل البطاقة في الصراف الآلي:

تعتمد عملية سحب الأموال أو تنفيذ العمليات عبر الصراف الآلي على تفاعل منظم بين البطاقة البنكية والنظام البنكي. يوضح هذا الشكل المراحل الرئيسية التي تمر بها البطاقة أثناء استخدامها في جهاز الصراف الآلي، بدءًا من إدخال البطاقة إلى تنفيذ العملية المطلوبة واستلام الإيصال أو النقود.

1.7. إدخال البطاقة:

يبدأ المستخدم العملية بإدخال بطاقته البنكية في فتحة مخصصة بجهاز الصراف الآلي.

2.7. قراءة بيانات البطاقة:

يقوم الجهاز بقراءة المعلومات المشفرة على الشريط المغناطيسي أو الشريحة الإلكترونية الموجودة على البطاقة.

3.7. إدخال الرمز السري (PIN)

يُطلب من المستخدم إدخال رقمه السري للتحقق من هويته بشكل آمن.

4.7. التحقق من البيانات

يقوم الجهاز بإرسال المعلومات إلى النظام البنكي للتحقق من صحتها وصلاحيّة البطاقة.

5.7. اختيار نوع العملية

بعد التحقق، يُمنح المستخدم إمكانية اختيار نوع الخدمة المطلوبة مثل السحب النقدي أو الاستعلام عن الرصيد.

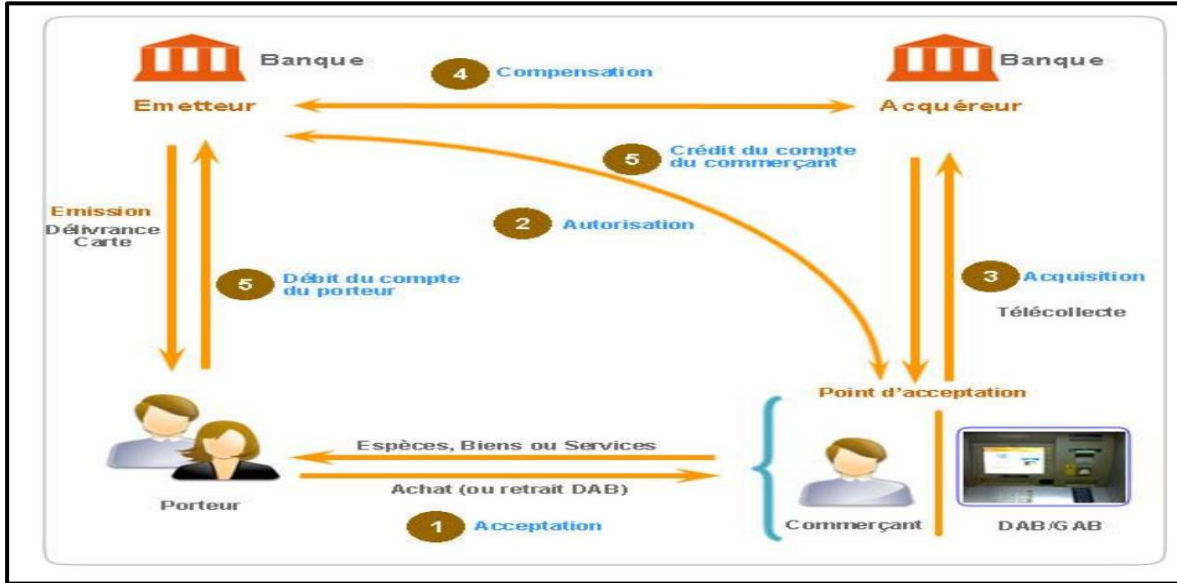
6.7. تنفيذ المعاملة

يتم تنفيذ العملية المطلوبة بعد الحصول على الموافقة من البنك أو مركز المعالجة (SATIM).

7.7. تسليم النقود أو الإيصال

في حال السحب، يخرج الجهاز المبلغ المطلوب، كما تتم طباعة وصل يوضح تفاصيل العملية. يوضح الشكل 10 المراحل التي تمر بها البطاقة البنكية أثناء استخدامها في جهاز الصراف الآلي يعرض هذا الشكل التسلسل الزمني للخطوات المتبعة من إدخال البطاقة إلى تنفيذ المعاملة واسترجاع البطاقة، مما يضمن الأمان والكفاءة في التعامل مع العمليات المالية بشكل سلس وآمن.

الشكل 10: يوضح الشكل مراحل عمل البطاقة في الصراف الألي



المصدر: Université d'Alger 3. (2019). Les technologies de l'information et de la communication avec les perspectives d'amélioration des opérations bancaires .Mémoire de Master, Université d'Alger 3. p. 46

المطلب الثاني: تصنيف وتحليل المخاطر الخاصة ببطاقات الدفع

1. تحليل المخاطر التشغيلية المرتبطة ببطاقات الدفع البنكية:

1.1. تعريف المخاطر التشغيلية في بطاقات الدفع البنكية:

المخاطر التشغيلية هي المخاطر الناتجة عن فشل الأنظمة، الأخطاء البشرية، أو عمليات الاحتيال أثناء استخدام بطاقات الدفع البنكية (BCBS, 2011).

تتضمن هذه المخاطر الأخطاء التقنية، عمليات الاحتيال، والهجمات الإلكترونية التي قد تؤثر على موثوقية وأمان العمليات المالية.

2.1. تصنيف المخاطر التشغيلية في بطاقات الدفع البنكية:

تتعدد المخاطر التشغيلية المرتبطة باستخدام بطاقات الدفع البنكية، ويمكن تصنيفها وفقاً لأنواع مختلفة تؤثر على الأمان والكفاءة في إجراء المعاملات المالية.

1.2.1. مخاطر الاحتيال والاختراقات الأمنية

تشمل عمليات الاحتيال التي تستهدف بطاقات الدفع البنكية من خلال:

– الاحتيال عبر سرقة البيانات (Phishing): يتم خداع المستخدمين لإدخال بيانات بطاقاتهم في مواقع احتيالية (Mishra & Gupta, 2022).

– الهجمات السيبرانية: تشمل البرمجيات الخبيثة (Malware) وهجمات الاختراق التي تستهدف أنظمة الدفع (Osei & Agyemang, 2020).

– التزوير المغناطيسي (Skimming): يتم نسخ بيانات البطاقة باستخدام أجهزة خاصة مثبتة على أجهزة الصراف الآلي أو نقاط البيع (Nguyen & Tran, 2019).

2.2.1. المخاطر التقنية والنظامية

تتعلق بأداء واستمرارية عمل أنظمة الدفع وتشمل:

– الأعطال التقنية: مثل فشل أنظمة المعالجة الفورية للمدفوعات مما يؤدي إلى تأخير أو فشل العمليات (Agarwal & Dhar, 2014).

– انقطاع الشبكة أو الاتصال: قد يؤدي إلى عدم القدرة على تنفيذ العمليات المالية في نقاط البيع أو عبر الإنترنت (Bouras & Khelifi, 2019).

– أخطاء البرمجة: قد تؤدي إلى خصم غير صحيح أو معاملات مكررة (Zhang & Wang, 2019).

3.2.1. مخاطر الامتثال والتنظيم

تنشأ بسبب عدم الامتثال للمعايير المصرفية والقوانين المالية:

– عدم الامتثال لقوانين مكافحة غسيل الأموال (AML): قد يؤدي إلى فرض غرامات على

المؤسسات المالية (Zarif & Hossain, 2020).

– عدم اتباع معايير أمان الدفع (PCI-DSS):

قد يعرض بيانات العملاء لخطر السرقة (Mebarki & Benali, 2022).

– الاختلاف في التشريعات الدولية: يؤدي إلى تعقيدات قانونية عند استخدام البطاقات في دول

مختلفة (Arora & Rahman, 2018).

3.1. استراتيجيات الحد من المخاطر التشغيلية:

تعتبر استراتيجيات الحد من المخاطر التشغيلية ضرورية لضمان أمان وكفاءة استخدام بطاقات الدفع

البنكية. ويمكن تصنيف هذه الاستراتيجيات وفقاً لتدابير وقائية وتقنيات تهدف إلى تقليل تأثير المخاطر

المحتملة

1.3.1. تعزيز الأمن السيبراني:

– استخدام تقنيات التشفير ثنائي العامل (FA2) للحماية من الاحتيال (BCBS, 2011).

– تطوير أنظمة كشف الاحتيال باستخدام الذكاء الاصطناعي (Mishra & Gupta, 2022).

تعزيز الوعي الأمني بين المستخدمين للحد من الهجمات الاحتيالية (Nguyen & Tran, 2019).

2.3.1. تحسين البنية التحتية التقنية: (Bouras & Khelifi, 2019).

– تطوير أنظمة احتياطية لتجنب فشل المعاملات بسبب انقطاع الخدمة

3.3.1. الامتثال للمعايير المصرفية والقانونية:

– الالتزام بمعايير أمان الدفع الإلكتروني (Zarif & Hossain, 2020) (PCI-DSS).

تحديث السياسات الداخلية لمكافحة غسيل الأموال والاحتيال المالي (Arora & Rahman, 2018)

2. أهمية خريطة المخاطر في قطاع بطاقات الدفع:

تساعد خريطة المخاطر في:

– تحليل المخاطر التشغيلية والأمنية المتعلقة باستخدام بطاقات الدفع.

– تحديد الأولويات بحيث يتم التعامل مع المخاطر الأكثر تهديدًا أولاً

(Nguyen & Tran, 2019).

– تحسين كفاءة استراتيجيات الحماية من خلال توزيع الموارد بشكل فعال وفقاً لمستوى المخاطر.

تعزيز الامتثال للمعايير الأمنية مثل PCI-DSS و ISO 27001 (Zarif & Hossain, 2020)

3. أنواع المخاطر في بطاقات الدفع البنكية وفق خريطة المخاطر:

تُعد بطاقات الدفع البنكية وسيلة فعالة لتسهيل المعاملات، لكنها تواجه عدة مخاطر تستدعي التحليل والتصنيف وتُستخدم خريطة المخاطر كأداة لتحديد هذه التهديدات وتقدير أثرها واحتمالية حدوثها يعرض هذا الجزء أهم أنواع المخاطر المرتبطة باستخدام البطاقات البنكية وفقاً لهذا النهج.

حيث يمكن تصنيف المخاطر إلى أربعة أقسام وفقاً لخريطة المخاطر:

الجدول رقم 4 : أنواع المخاطر في بطاقة الدفع البنكية

نوع الخطر	احتمالية الحدوث	درجة التأثير	الإجراءات الوقائية
الاحتيال الإلكتروني (Phishing,) (Skimming)	عالية	عالية	استخدام تقنيات التشفير ثنائي العامل وتوعية العملاء بمخاطر الاحتيال (Mishra & Gupta, 2022)
الهجمات السيبرانية (Cyber Attacks)	متوسطة	مرتفعة	تطبيق أنظمة كشف الاحتيال وتعزيز الأمن السيبراني (Osei&Agyemang 2020)
الأعطال التقنية (System) (Failures)	منخفضة	متوسطة	تطوير أنظمة احتياطية وخطط استمرارية الأعمال (Bouras & Khelifi, 2019).
عدم الامتثال للمعايير التنظيمية	منخفضة	مرتفعة	ضمان التوافق مع القوانين المصرفية ومعايير أمن الدفع الإلكتروني (Zhang & Wang, 2019).

المصدر: Mishra & Gupta, 2022; Osei & Agyemang, 2020; Bouras & Khelifi, 2019;

Zhang & Wang, 2019

المطلب الثالث: المنهجية الفعالة لتطبيق خارطة مخاطر بطاقات الدفع

1. المنهجية الفعالة لتطبيق خريطة المخاطر من أجل تعزيز أمان بطاقات الدفع:

يُعد اعتماد منهجية فعالة لتطبيق خريطة المخاطر أمراً حيوياً في تعزيز أمن بطاقات الدفع، خاصة في ظل تنامي التهديدات المرتبطة بالتحول الرقمي. إذ تتيح هذه الخريطة فهماً دقيقاً لمصادر الخطر ومواطن الضعف، مما يساعد المؤسسات المصرفية على اتخاذ قرارات استباقية، وتطوير آليات رقابة ملائمة تحدّ من احتمالات الاختراق أو الفشل التشغيلي.

1.1 تحديد المخاطر الأكثر تهديداً (Nguyen & Tran, 2019)

يتم تصنيف المخاطر وفقاً لمصفوفة المخاطر لتحديد النقاط الحرجة التي يجب معالجتها على الفور، مثل عمليات الاحتيال الإلكتروني التي تمثل تهديداً عالي الخطورة

2.1 تحسين استراتيجيات الاستجابة للمخاطر: (Mishra & Gupta, 2022).

تطوير أنظمة أمنية متقدمة تعتمد على الذكاء الاصطناعي لاكتشاف العمليات المشبوهة

تعزيز التعاون مع الهيئات التنظيمية لضمان الامتثال للقوانين المصرفية (Zarif & Hossain, 2020).

تدريب الموظفين والعملاء على اكتشاف الاحتيال والتعامل مع المخاطر الأمنية

(Osei & Agyemang, 2020).

3.1 مراقبة المخاطر بشكل مستمر

تنفيذ تحليلات البيانات الضخمة (Big Data Analytics) لمراقبة أنماط السلوك غير الطبيعي في

المعاملات المالية (Mebarki & Benali, 2022).

استخدام التعلم الآلي (Machine Learning) في تقييم مخاطر الاحتيال وتحليل سلوك المستخدمين

(Zhang & Wang, 2019).

4.1. نتائج تطبيق خريطة المخاطر في بطاقات الدفع:

- تقليل نسبة عمليات الاحتيال الإلكتروني بنسبة تصل إلى **40%** بفضل أنظمة الذكاء الاصطناعي (Mishra & Gupta, 2022).
- تحسين سرعة الاستجابة للهجمات السيبرانية وخفض تأثيرها بنسبة **30%** من خلال تطبيق استراتيجيات أمان استباقية (Osei & Agyemang, 2020) الامتثال لمعايير **PCI-DSS** و **ISO 27001** مما يرفع من موثوقية أنظمة الدفع البنكية ويعزز ثقة العملاء (Zarif & Hossain 2020).

المطلب الرابع : المخاطر التشغيلية الكامنة الخاصة ببطاقات الدفع البنكية

1. المخاطر التشغيلية الكامنة الخاصة ببطاقات الدفع البنكية:

تواجه بطاقات الدفع البنكية مجموعة من المخاطر التشغيلية التي تتجم عن خلل في الأنظمة، أو أخطاء بشرية، أو إخفاقات في الإجراءات الداخلية. وتكمن أهمية تحليل هذه المخاطر في قدرتها على التأثير المباشر على ثقة العملاء وسلامة المعاملات المالية يُعالج هذا المحور أبرز أوجه المخاطر التشغيلية المتعلقة ببطاقات الدفع، مع التركيز على مصادرها وآثارها المحتملة داخل السياق البنكي.

الجدول رقم 5: المخاطر التشغيلية المرتبطة ببطاقة الدفع البنكية

التوثيق	الوصف	الخطر التشغيلي
(Tarbikafa, 2016)	قيام موظفين باختلاس أموال أو التلاعب بالبيانات المالية.	الاحتيال المالي والاختلاس
(Tarbikafa, 2016)	استخدام وثائق مزورة لإجراء معاملات غير قانونية.	تزوير الشيكات والمستندات
(Tarbikafa, 2016)	تعرض الفروع أو أجهزة الصراف الآلي للسرقة.	السرقة والسطو
(.LP Centre, n.d)	هجمات سيبرانية تستهدف أنظمة الدفع لسرقة المعلومات أو الأموال.	الجرائم الإلكترونية
(.LP Centre, n.d)	فشل الأنظمة أو الأجهزة مما يؤدي إلى توقف الخدمات.	أعطال تقنية
(Tarbikafa, 2016)	أخطاء غير مقصودة من الموظفين تؤدي إلى خسائر مالية.	أخطاء بشرية
(.LP Centre, n.d)	عدم الالتزام باللوائح والقوانين مما قد يؤدي إلى عقوبات.	عدم الامتثال للمعايير
(Tarbikafa, 2016)	محاولات خداع العملاء للحصول على معلوماتهم السرية.	هجمات التصيد الاحتمالي

تابع للجدول أعلاه ص 97.

(.LP Centre, n.d)	تركيب أجهزة غير شرعية لسرقة بيانات البطاقات	استخدام أجهزة الصراف الآلي المزيفة
(Tarbikafa, 2016)	كشف غير مصرح به للمعلومات الحساسة للعملاء.	تسريب البيانات
(.LP Centre, n.d)	توقف الخدمات بسبب فقدان الطاقة الكهربائية.	انقطاع التيار الكهربائي
(Tarbikafa, 2016)	أحداث طبيعية تؤثر على البنية التحتية للأنظمة المصرفية.	الكوارث الطبيعية
(Tarbikafa, 2016)	عدم كفاية تدريب الموظفين مما يؤدي إلى أخطاء تشغيلية.	نقص التدريب للموظفين
(.LP Centre, n.d)	أنظمة قديمة أو غير متطورة تزيد من مخاطر الأعطال.	ضعف البنية التحتية التقنية
(.LP Centre, n.d)	إغراق الخوادم بالطلبات لتعطيل الخدمات.	هجمات حجب الخدمة (DDoS)
(Tarbikafa, 2016)	برامج ضارة تستهدف أنظمة الدفع لسرقة البيانات.	البرمجيات الخبيثة
(.LP Centre, n.d)	ضياع أو سرقة أجهزة تحتوي على معلومات حساسة.	فقدان الأجهزة المحمولة
(Tarbikafa, 2016)	إجراءات أمنية غير كافية لحماية الأنظمة والبيانات.	ضعف سياسات الأمان
(.LP Centre, n.d)	قرارات الموظفين التي تفيد مصالحهم الشخصية على حساب المؤسسة	تعارض المصالح
(.Interpol, n.d)	استخدام مواقع وهمية لسرقة بيانات البطاقات.	الاحتيال عبر الإنترنت
(.Interpol, n.d)	إرسال أوامر مباشرة إلى أجهزة الصراف الآلي لسحب الأموال.	هجمات "الصندوق الأسود"
SAMA Rulebook,) (.n.d	عدم وجود سياسات فعالة لإدارة المخاطر التشغيلية.	ضعف إدارة المخاطر

تابع للجدول أعلاه ص 98.

(CBE, 2021)	تطبيقات مزيفة تهدف لسرقة بيانات المستخدمين.	الاحتيال في تطبيقات الهواتف المحمولة
(AMF, 2022)	تأثير الأحداث السلبية على سمعة المؤسسة.	مخاطر السمعة
(CBE, 2021)	استغلال خدمات الدفع الهاتفي للاحتيال.	الاحتيال في خدمات الدفع عبر الهاتف المحمول

المصدر: من إعدادنا الشخصي

الفصل الثاني: الإطار الميداني و المنهجي

المبحث الأول: مؤسسة الدراسة

يُشكّل هذا المحور جزءاً جوهرياً من الدراسة إذ يسلط الضوء على السياق العملي الذي تم فيه إجراء البحث من خلال تقديم المؤسسة المضيفة وهي بنك ترست الجزائر باعتبارها نموذجاً حيويّاً لفهم الممارسات المصرفية المرتبطة بإدارة المخاطر التشغيلية.

كما يعرض هذا المحور الأسس المنهجية التي تم اعتمادها في جمع وتحليل البيانات والتي تُعد ضرورية لضمان المصادقية والدقة العلمية للنتائج المتوصّل إليها.

يتضمن المحور تعريفاً شاملاً لبنك ترست الجزائر من حيث النشأة البنية القانونية مسار التطور وتوجهاته الاستراتيجية في الابتكار والتوسع مما يبرز اختياره كمجال للدراسة الميدانية بالنظر إلى موقعه الريادي في السوق المصرفية الجزائرية.

ثم ينتقل المحور إلى عرض المنهجية النوعية المتبعة في هذا البحث حيث تم تبني مقاربة بنائية تعتمد على أدوات مثل المقابلات وتحليل الوثائق لفهم وتقييم المخاطر التشغيلية المرتبطة ببطاقات الدفع البنكية.

هذه المنهجية تندرج ضمن إطار إبستمولوجي بنائي يركّز على الملاحظة الموضوعية والتحليل المنهجي للظواهر ما يُضفي على نتائج الدراسة طابعاً علمياً قابلاً للتعميم.

المطلب الأول: تقديم المؤسسة المستقبلة - بنك ترست الجزائر

1. تقديم مؤسسة الدراسة - بنك ترست الجزائر:

1.1. التعريف بالمؤسسة: (Rapport d'activité 2021)

بنك ترست الجزائر (Trust Bank Algeria) هو مؤسسة بنكية خاصة رائدة في السوق المصرفية

الجزائرية يتميز بـ:

الشكل القانوني: شركة ذات أسهم (SPA)

المقر الاجتماعي: 17 شارع العربي عليك - حيدرة - الجزائر العاصمة

الانتماء: عضو في مجموعة "نيست إنفستمننتس هولدينغ" القبرصية

التصنيف: بنك تجاري شامل يقدم خدمات مصرفية تقليدية وإسلامية

رأس المال: 20 مليار دينار جزائري (2021)

الشبكة: 35 فرعاً منتشرة عبر التراب الوطني

2.1. النشأة والتطور التاريخي: (Rapport d'activité 2021)

المراحل الرئيسية في تطور البنك:

مرحلة التأسيس (2003):

- بدء النشاط في أبريل 2003 برأس مال أولي 750 مليون دج

- التركيز الأولي على الخدمات المصرفية الأساسية

- مرحلة التوسع (2012-2015):

- زيادة رأس المال إلى 13 مليار دج عام 2012

- تطوير شبكة الفروع وخدمات الشركات

- مرحلة النضج (2016-2020):

- إطلاق الخدمات المصرفية الإسلامية

- بدء التحول الرقمي

- مرحلة التميز (2021-الآن):

- زيادة رأس المال إلى 20 مليار دج

- تطوير خدمات التمويل المتخصصة

- تعزيز البنية التحتية التكنولوجية

3.1. الابتكار في الخدمات المصرفية

رائد في تقديم الحلول المصرفية الإسلامية

من أوائل البنوك في تبني التقنيات المالية الحديثة

تطوير منتجات مالية مبتكرة تلبى احتياجات جميع الشرائح

4.1. المؤشرات الرئيسية (2021):

الجدول رقم 6: المؤشرات الرئيسية لبنك تراست

المؤشر	القيمة
حجم الأصول	138 مليار دج
صافي الربح	5 مليار دج

المصدر. Trust Bank Algeria. (2021). Rapport d'activité 2021. <https://www.trustbankalgeria.com> (Consulté le 16/04/2025)

5.1. الاعترافات والجوائز. (Rapport d'activité 2021)

– جائزة أفضل بنك في الخدمات الرقمية (2020)

– شهادة التميز في الخدمات المصرفية الإسلامية (2021)

– تصنيف A+ من وكالة "موديز" للتصنيف الائتماني

– المساهمة الفاعلة في تحقيق أهداف التنمية المستدامة

المطلب الثاني : الهيكل التنظيمي والخصائص التشغيلية لبنك تراست الجزائر

1. الهيكل الإداري: (Rapport d'activité 2021)

يتكون مجلس إدارة البنك من عدة أعضاء، ويرأسه غازي كامل أبو ناهل، بينما يشغل شيخ

ناصر بن علي آل ثاني منصب نائب الرئيس. كما يضم عدة لجان رقابية وإدارية مثل:

– لجنة التدقيق (Audit Committee)

– لجنة المخاطر (Risk Committee)

– لجنة التعويضات والمكافآت (Compensation Committee)

1.1 . الأنشطة والخدمات.: (Rapport d'activité 2021)

بنك تراست الجزائر يعمل كبنك شامل ويقدم مجموعة من الخدمات المصرفية، منها:

- التمويل التجاري (Corporate Finance)
- الخدمات المصرفية للأفراد (Retail Banking)
- التمويل الإسلامي (Trust Ijara)
- الخدمات المصرفية الرقمية (TBA Net & Mobile Banking)
- تسهيلات الدفع الإلكتروني (بطاقات CIB، Visa، Mastercard)

2.1 . الحضور الجغرافي.: (Rapport d'activité 2021)

يملك البنك أكثر من 35 فرعًا في مختلف أنحاء الجزائر مع خطط مستمرة لتوسيع شبكته لتعزيز الخدمات المالية والقرب من العملاء.

3.1 . الأداء المالي:

حقق البنك في 2021 نتائج إيجابية، حيث بلغ إجمالي الميزانية 138.4 مليار دينار جزائري، مع صافي أرباح بلغ 5.01 مليار دينار جزائري، ونسبة نمو في الودائع بلغت 75.73% مقارنة بالسنة السابقة.

2. الهيكل التنظيمي والإداري: (Rapport d'activité 2021)

1.2. الإدارة العامة لبنك تراست الجزائر:

1.1.2. مجلس الإدارة

يضم مجلس إدارة بنك تراست الجزائر (TBA) شخصيات مصرفية واستثمارية بارزة تعمل على توجيه

استراتيجيات البنك وتحديد سياساته العامة. يرأس المجلس:

- غازي كامل أبو نهل - رئيس مجلس الإدارة.
- شيخ ناصر بن علي آل ثاني - نائب رئيس مجلس الإدارة.
- بالإضافة إلى عدد من الأعضاء من ذوي الخبرة في مجالات التمويل، الاستثمار، المخاطر، والتكنولوجيا المالية.

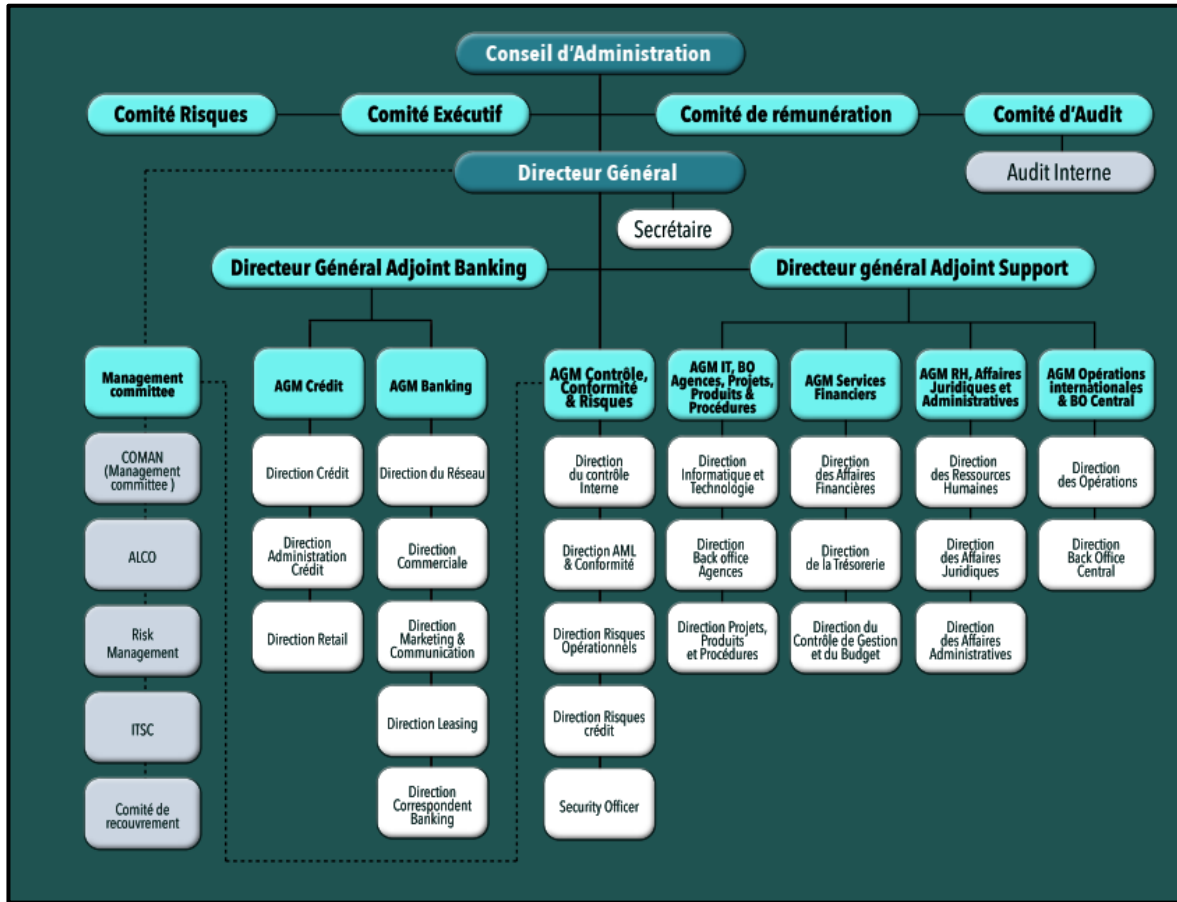
2.1.2. الإدارة التنفيذية:

تتولى الإدارة التنفيذية مسؤولية الإشراف اليومي على العمليات المصرفية، وتوجيه أنشطة البنك بما

يتماشى مع استراتيجيات مجلس الإدارة. وتتكون من:

- المدير العام: مسؤول عن التنفيذ العام لاستراتيجية البنك وإدارة عملياته اليومية.
- نائب المدير العام: يساعد المدير العام في الإشراف على الإدارات المختلفة وضمان تنفيذ الخطط.

الشكل 11: الهيكل التنظيمي لبنك تراست



المصدر: Trust Bank Algeria. (2021). Rapport d'activité 2021.

<https://www.trustbankalgeria.com> (Consulté le 16/04/2025)

المطلب الثالث : الأنشطة والخدمات المصرفية

3. الأنشطة والخدمات المصرفية: (Rapport d'activité 2021)

1.3. الحسابات والخدمات البنكية

يقدم بنك تراست الجزائر مجموعة متنوعة من الحسابات المصرفية المصممة لتلبية احتياجات الأفراد

والشركات، وتشمل:

– الحسابات الجارية: مخصصة للمعاملات اليومية، مع إمكانية إصدار دفتر شيكات وبطاقات

خصم.

- حسابات التوفير: توفر فوائد تنافسية مع إمكانية الوصول إلى الأموال بسهولة.
- الحسابات بالعملة الصعبة: مخصصة للعملاء الذين يتعاملون بالدولار أو اليورو، مما يسهل عمليات التجارة والتحويلات الدولية.
- حسابات المؤسسات والشركات: توفر حلولاً مصرفية مرنة للشركات، مثل الحسابات متعددة العملات وإدارة السيولة.

2.3. القروض والتمويلات

يقدم البنك حلولاً تمويلية متنوعة للأفراد والشركات، من بينها:

- القروض الاستهلاكية: تشمل قروض شراء السيارات، القروض الشخصية، وتمويل المشاريع الصغيرة.
- التمويل العقاري: يشمل القروض السكنية لشراء المنازل أو تجديد العقارات.
- القروض الاستثمارية: مصممة لدعم الشركات في توسيع أعمالها وتمويل المشاريع الكبرى.
- التمويل الإسلامي: يوفر البنك خيارات مثل المرابحة، الإجارة، والمضاربة كبداية للقروض التقليدية.

3.3. الخدمات الرقمية والمصرفية عبر الإنترنت: (Rapport d'activité 2021)

- يواكب بنك تراست الجزائر التحول الرقمي من خلال تقديم مجموعة من الخدمات الإلكترونية، ومنها:
- التطبيق البنكي: يتيح للعملاء إدارة حساباتهم، دفع الفواتير، وتحويل الأموال عبر الهواتف الذكية.

- الخدمات المصرفية عبر الإنترنت: تشمل الاطلاع على الرصيد، تنفيذ المعاملات، والتحكم في البطاقات البنكية.

- لدفع الإلكتروني: يدعم الدفع عبر QR Code، والمحافظ الرقمية، وخدمات الدفع الإلكتروني المحلية والدولية.

- ماكينات الصراف الآلي (ATM): تقدم خدمات السحب والإيداع والتحويل بين الحسابات بسهولة

4.3. الحسابات والخدمات البنكية (أرقام 2021)

الجدول رقم 7: أنواع الحسابات في تراست بنك

نوع الحساب	عدد الحسابات	حجم الودائع (مليار دينار)	معدل النمو السني
الحسابات الجارية	185,320	48.7	12+%
حسابات التوفير	92,450	32.4	18+%
الحسابات الإسلامية	43,210	15.2	25+%

المصدر: Trust Bank Algeria. (2021). Rapport d'activité 2021

<https://www.trustbankalgeria.com> (Consulté le 16/04/2025)

4. خدمات التحويلات: (Rapport d'activité 2021)

حجم التحويلات المحلية: 4.2 مليون عملية سنوياً (+22% عن 2022)

عمليات الصراف الآلي: 8.7 مليون عملية/سنوياً

5. الخدمات الرقمية (إحصاءات 2023)

- عمليات الدفع الإلكتروني: 3.8 مليون عملية (1.2 مليار دج)

- فتح الحسابات عن بعد: 12,340 حساب (27% من إجمالي الجدد)

- نسبة رضا العملاء: 5/4.6 (وفق استطلاع Q3 - 2023)
- تظهر هذه الأرقام قدرات بنك ترست في:
- نمو محفظة التمويل الإسلامي (+25% سنوياً)
- كفاءة القنوات الرقمية (38% من العمليات
- مع استراتيجية واضحة لتحقيق:
- نجاح تطبيق **Trust Connect** (زيادة استخدام الخدمات عبر الهاتف بنسبة 40%)
- 50% حصة للخدمات الرقمية بحلول 2025
- 15% نمو سنوي في محفظة التمويل
- 20% زيادة في قاعدة العملاء سنوي
- مشروع إطلاق خدمات جديدة مثل:
- الدفع عبر QR Code.
- فتح الحسابات عن بُعد.

المبحث الثاني :المنهجية البحثية

يُعد الإطار المنهجي من الركائز الأساسية لأي بحث علمي حيث يحدد الأسس المنهجية التي يعتمد عليها الباحث في دراسة الظاهرة محل البحث.

يهدف هذا الفصل إلى توضيح المقاربة الأبيستمولوجيا التي تم تبنيها بالإضافة إلى المنهجية المعتمدة وأدوات البحث المستخدمة في جمع وتحليل البيانات يساعد هذا الإطار على ضمان الدقة والموضوعية في معالجة الإشكالية المطروحة مما يسهم في الوصول إلى نتائج موثوقة وقابلة للتطبيق.

في هذا السياق سيتم في هذا الفصل استعراض الموقف الأبيستمولوجيا الذي يوجه البحث وتحديد نوع المنهجية المتبعة سواء كانت كمية أو نوعية بالإضافة إلى الأدوات والتقنيات المستخدمة في جمع البيانات مثل المقابلات تحليل الوثائق والملاحظات الميدانية كما سيتم توضيح كيفية تحليل المعطيات من أجل الوصول إلى استنتاجات تسهم في فهم الظاهرة المدروسة واقتراح حلول مناسبة له

المطلب الأول : الموقف الأبيستمولوجيا وطريقة البحث

1.الموقف الأبيستمولوجيا وطريقة البحث

1.1. الموقف الأبيستمولوجيا: IOR, 2010 (؛ Bessis, 2015؛ Bellini, 2016)

تُعد منهجية التقييم الذاتي للمخاطر والرقابة (RCSA - Risk and Control Self-Assessment) إطارًا تشغيليًا منهجيًا وتشاركيًا يُستخدم لتحديد وتقييم وإدارة المخاطر التشغيلية داخل المؤسسات من خلال إشراك أصحاب العمليات - من موظفين ومديرين - في تحليل المخاطر المرتبطة بأنشطتهم وتقييم مدى فعالية الضوابط الرقابية المعتمدة مع تحديد الفجوات ووضع خطط عمل تصحيحية عند الحاجة. وتهدف هذه المنهجية إلى تمكين الخط الأول للدفاع من تحمّل مسؤولية إدارة المخاطر الواقعة ضمن نطاقهم، وتعزيز الوعي المؤسسي بالمخاطر وترسيخ ثقافة الرقابة والمساءلة على مختلف المستويات.

كما تسهم في تحقيق التكامل بين أهداف المؤسسة وبيئتها التشغيلية، وتدعم الامتثال للمعايير الدولية وأطر الحوكمة مثل إطار COSO (2013)، وتوصيات لجنة بازل (2015, 2011, BCBS)، ومعيار ISO 31000 وتُعد RCSA أداة استباقية تُنفَّذ بشكل دوري لتحديد المخاطر الكامنة والمخاطر المتبقية، وقياس مدى كفاءة البيئة الرقابية، سواء بأسلوب نوعي أو كمي، ما يجعلها ركيزة أساسية في أنظمة إدارة المخاطر وفي تحسين فعالية التدقيق الداخلي وصنع القرار المؤسسي.

2.1. طريقة البحث:

تعتمد هذه الدراسة في معالجة موضوع المخاطر التشغيلية على تطبيق منهجية RCSA كإطار تحليلي نوعي يدمج بين الفهم الميداني العميق والتقييم الذاتي المنظم.

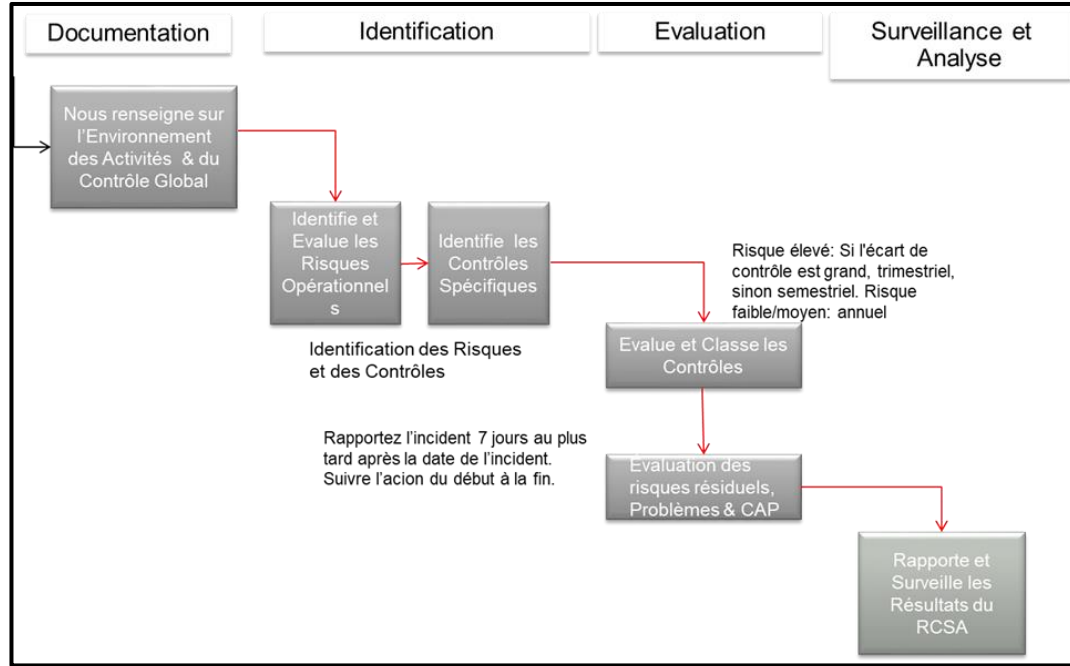
وقد تم اختيار هذه المنهجية نظرًا لكونها أداة فعالة لتحديد وتقييم الضوابط الداخلية والمخاطر المرتبطة بالأنشطة التشغيلية، من خلال إشراك المعنيين بشكل مباشر في بيئة العمل، مثل الموظفين ومديري الأقسام، في تحليل المخاطر وتحديد الثغرات ووضع خطط عمل لمعالجتها (IOR, 2010).

وتقوم عملية البحث، وفقًا لمنهجية RCSA، على سلسلة خطوات منهجية تبدأ بتحديد الأهداف التشغيلية للوظيفة أو العملية محل الدراسة، تليها مرحلة تحديد المخاطر المحتملة التي قد تعيق تحقيق هذه الأهداف، ثم تحليل الضوابط الرقابية الموجودة ومدى فعاليتها من حيث التصميم والتنفيذ.

بعد ذلك يتم تقييم مستوى المخاطر المتبقية، أي المخاطر التي لا تزال قائمة رغم وجود الضوابط، وتصنيفها حسب الأولوية باستخدام أدوات تحليلية مثل مصفوفات الاحتمال والتأثير. كما يشمل البحث إعداد خطط عمل تصحيحية (Action Plans) لمواجهة الفجوات الرقابية وتوثيقها في سجلات رسمية، مع تحديد المسؤوليات والجداول الزمنية للمتابعة.

الشكل الموالي يوضح منهجية إدارة المخاطر التشغيلية من خلال التقييم الذاتي للمخاطر و الضوابط

الشكل 12: منهجية إدارة المخاطر التشغيلية من خلال التقييم الذاتي للمخاطر والضوابط (RCSA)



المصدر: [de travail, Trust Bank Algérie].

وقد اعتمد هذا البحث على الورشة التفاعلية (Workshop-Based RCSA) بوصفها المنهج الأنسب للسياق محل الدراسة، نظرًا لما توفره من بيئة تشاركية ومرنة تسمح بتبادل وجهات النظر، وتحفيز التفكير الجماعي في تقييم المخاطر والضوابط بشكل واقعي (IOR, 2010؛ Bellini, 2016). وتمت جدولة الورشات وفق مقارنة تدريجية انطلقت من المستوى التنفيذي نحو المستويات التشغيلية، مع مراعاة إشراك أصحاب العلاقة، ومسير محايد (facilitator) في حالة بنك تراست المحايد هو مدير المخاطر التشغيلية الذي يشرف على تسير الورشات، إعتدنا على أدوات تكنولوجية ومن الأمثلة على هذه الأدوات المستخدمة في إدارة المخاطر في البنك تطبيق Risk Nucleus هو تطبيق لإدارة المخاطر يستخدمه بنك تراست تحديد وتقييم المخاطر المحتملة التي قد تؤثر على عمليات البنك.

يُتيح التطبيق للبنك مراقبة المخاطر في الوقت الفعلي، تحليل البيانات، التنبؤ بالمخاطر المستقبلية، وتطوير استراتيجيات استجابة لتقليل هذه المخاطر. كما يوفر تقارير شاملة تساعد في اتخاذ قرارات مستنيرة لتعزيز أمان العمليات البنكية وضمان الامتثال للوائح القانونية.

يبين الشكل التالي طريقة إعداد ورشة في تطبيق Risk Nucleus:

الشكل 13: يوضح الشكل واجهة إعداد ورشات العمل في تطبيق Risk Nucleus

ID	Intitulé	Directeur d'entité	Coordinateur des risques	Entité	Matrice	Date	Statut	Nombre de Risques	Nombre de Contrôles	Nombre de Plans D'action
WS3110				Direction Informatique et Technologie	TBA Global Matrix	20 Oct 2024	Not Started	7	0	0
WS3109				Direction du Contrôle des Opérations	TBA Global Matrix	07 Oct 2024	Not Started	1	0	0
WS3108				Département Monétique	TBA Global Matrix	18 Sep 2024	In progress	1	0	0
WS2109				Direction des Affaires Administratives	TBA Global Matrix	23 Apr 2024	Not Started	2	0	0
WS2106				Direction Back Office Opérations Agences	TBA Global Matrix	23 Apr 2024	In progress	12	0	0
WS2098				Direction du Contrôle de Gestion et du Budget	TBA Global Matrix	24 Jun 2021	In progress	1	0	0
WS2097				Direction Administration Crésit	TBA Global Matrix	24 Jun 2021	In progress	0	0	0
WS2096				Direction Marketing et Communication	TBA Global Matrix	27 Jun 2021	In progress	0	0	0
WS2095				Direction des Affaires Financières	TBA Global Matrix	24 Jun 2021	In progress	2	0	0
WS2094				Direction Projets, Produits et Procédures	TBA Global Matrix	23 Jun 2021	In progress	0	0	0

المصدر: تطبيق Risk Nucleus تراست بنك

يعرض الشكل 13 واجهة إعداد ورشة عمل RCSA من خلال نظام RISK NUCLEUS. عند النقر على زر "إضافة ورشة جديدة"، تظهر نافذة منبثقة تتضمن مجموعة من الحقول الأساسية مثل: عنوان الورشة، الجهة المعنية (مثلاً: مديرية تكنولوجيا المعلومات أو المديرية النقدية)، المصنوفة المعتمدة، التاريخ، ومدير الورشة ومنسق المخاطر.

تتيح هذه الواجهة للمستخدم تنظيم ورش العمل الخاصة بتقييم المخاطر والضوابط بشكل منسق وسهل، مع إمكانية حفظ المعلومات أو إلغاؤها حسب الحاجة.

الشكل 14: مضمون ورشة العمل في تطبيق Risk Nucleus

Workshop- Workflow												
Ajouter un nouveau risque Edit Risk Supprimer Risque Importer risque Exporter risque transfert d'atelier Carte de Chaleur Data Download Consolider les résultats Attribuer des risques												
Workshop Details Workshop Entity: Département Monétique Workshop Owner: NABIL Workshop Coordinator: NAF Workshop Capital: TBA Global Matrix Workshop Inherent Score: 2,790,004,000 Workshop Residual Score: 250,000,000 Workshop Target Score: 250,000,000						Workshop Participants SAMA LND WRE MEN WAMEL SAF						
Option de filtre												
Show 10 entries												
ID	Initial	Description	Evaluation inhérente	TA	Evaluation résiduelle	VOAC	Carte de Chaleur	Results	Statut	Nombre de Contrôles	Nombre de Plans D'action	Risk Response
R0K030		Affectation d'un TPE à deux clients différents				USD 200,000,000		Complete	0	0		
R0K036		Fichier des réclamations initial de Trust Card incomplet				USD 500,001,000		Complete	0	0		
R0K016		Marque de suivi et de prise en charge des réclamations sur TPE				USD 500,001,000		Complete	0	0		
R0K126		Transmission d'un fichier erroné, incomplet, ou en double à EMP				USD 500,001,000		Complete	0	0		

المصدر: تطبيق Risk Nucleus تراست بنك

يوضح الشكل التالي 14 واجهة نظام إدارة ورشة عمل تقييم المخاطر، والتي تُستخدم لتحديد وتحليل المخاطر المرتبطة بعملية معينة داخل البنك تتضمن الواجهة عدة وظائف تتيح للمستخدم إضافة المخاطر، تعديلها، تصديرها أو استيرادها، بالإضافة إلى أدوات تحليل مثل بطاقة الحرارة وتنزيل البيانات. هذا النظام يسهل عملية اتخاذ القرار عبر عرض معلومات دقيقة ومهيكله حول المخاطر، مما يعزز من فعالية إدارة المخاطر في البنك.

ومن أهم مميزات هذا التطبيق هو كمية التقارير والتي تعتبر النتيجة النهائية لورشات العمل سوف نتطرق

إلى أمثلة حول هذه التقارير في الشكل الموالي رقم (15)

الشكل 15: مختلف التقارير الآلية التي يمنحها Risk Nucleus

Report ID	Report Title	Report Description
RP12	Matrice 18 cellules	Incidents affichés par ligne de métier et par catégorie de risque, cartographiés sur une matrice de 18 cellules
RP13	Matrice incidents de 6ème	Par activité
RP14	Catégorie de risque	Incidents affichés par catégorie de risque
RP15	Catégorie de risque 2	Par activité
RP16	Catégorie de risque 3	Par activité
RP17	Incident particulier	Rapport de détail d'incident particulier avec description complète de l'incident
RP18	Résumé d'incidents	Rapports d'incidents multiples avec catégorie de risque, numéro de référence TIC et plan d'action
RP19	Résumé d'incident 2	Par activité
RP110	Plans d'action	Rapport de plan d'action 6ème par unité particulière
RP111	Plans d'action par priorités	Plans d'action par priorités, affichage à statut
RP112	Déclaration d'incident	Tous les formulaires de déclaration d'incident par statut et priorités
RP113	Résumé incidents	Par activité
RP114	Plans d'action	Rapport de plan d'action 6ème par unité, affiche le lien entre l'incident et l'indicateur de
RP115	Plans d'action par priorités	Plans d'action par priorités, affichage à statut
RP116	Déclaration d'incident	Tous les formulaires de déclaration d'incident par statut et priorités
RP117	Matrice	Incidents affichés par unité et par catégorie de risque. Cartographiés sur une matrice
RP118	Tendance des événements à risque	Affiche un graphique des événements à risque par mois et un tableau de incidents, 6ème par année, type de site et statut financier
RP119	Incidents avec plans d'action	Affiche tous les incidents associés à des plans d'action
RP120	Incidents avec des plans d'action en retard	Affiche tous les incidents associés à des plans d'action en retard
RP121	Personnel financier inclus GDF	Par activité
RP122	Tableaux	Tableaux
RP123	Capture Web	Capture Web
RP124	Rapport sur un seul incident	Rapport d'incident unique uniquement avec description de l'incident
RP125	Liste de rapports sur plusieurs incidents ensembles	Liste de rapports sur plusieurs incidents ensembles
RP126	Rapport de points pour tout type de montant	Rapport de points pour tout type de montant avec points pondérés
RP127	Liste de rapport continue de points en deux semaines	Liste de rapport continue de points en deux semaines
RP128	Liste des plans d'action 6ème	Affiche une liste de plans d'action 6ème par colonne
RP129	Cap Sheet	Cap Sheet
RP130	Pending DataPoint by Department	Points de données en attente par direction et par fournisseur
RP131	Des indicateurs with Risk by 60 scores	Indicateurs 60 avec scores de risque par 60
RP132	Tableau résumé par Risque Catégorie and Business Lines	Récapitulatif du montant de la perte par catégorie de risque et ligne métier
RP133	LCI segment report	LCI segment report
RP134	Operational Loss Data Summary by Segments	Operational Loss Data Summary by Segments
Fraud Management		
Report ID	Report Title	Report Description
RP135	Liste de formulaires de déclaration	Par activité
RP136	Formulaires de déclaration	Par activité
Risk & Control Self-Assessment		
Report ID	Report Title	Report Description
RP137	Profil des risques par unité	Affiche un graphique simple de répartition horizontale et de contrôle de réduction, avec quatre fils des risques 6ème par unité et statut
RP138	Profil des risques par unité 2	Affiche une liste des risques 6ème par unité, statut et unité de graphique simple
RP139	Profil des risques par unité 3	Affiche un diagramme à barres des approches horizontales, répartition et de contrôle, avec quatre fils des risques 6ème par unité, statut et unité à 3 barres
RP140	Profil des risques par unité 4	Affiche un graphique simple des données horizontales et de contrôle de réduction, avec quatre fils des risques 6ème par unité, statut, cartographie horizontale
RP141	Rapport des risques	Affiche une liste des risques 6ème par statut
RP142	Liste des conditions par risque	Affiche une liste de conditions par 60 de risque 6ème par unité ou par ligne de métier

المصدر: تطبيق Risk Nucleus تراست بنك

يُظهر الشكل 15 قائمة التقارير المتاحة ضمن نظام RISK NUCLEUS والتي تُستخدم في إطار إدارة وتتبع الحوادث المرتبطة بالمخاطر التشغيلية داخل البنك. تتضمن القائمة رمز التقرير، عنوانه، ووصفاً موجزاً لمحتواه أو الغرض منه وتتنوع التقارير بين مصفوفات تقييم الحوادث (مثل "مصفوفة 56 خلية")،

تصنيفات الأسباب، خطط العمل، وملخصات الحوادث، بالإضافة إلى تقارير تحليلية مثل اتجاهات الحوادث وتصنيفها حسب الكيان أو الحالة.

توفر هذه التقارير أدوات تحليل متعددة تساعد في تتبع الحوادث وفهم أنماط تكرارها وأسبابها، كما تدعم عملية اتخاذ القرار من خلال تقديم رؤية واضحة حول النقاط الحرجة داخل العمليات البنكية التي قد تحتاج إلى تدخل أو إجراءات تصحيحية.

المطلب الثاني: النموذج التحليلي

1. نموذج التحليل:

ولقد اعتمدنا في دراستنا لتحليل المخاطر التشغيلية المرتبطة ببيئة الدفع البنكي على منهجية التقييم الذاتي للمخاطر والرقابة (RCSA)، وذلك باستخدام نموذج تحليلي مبني على النظام اللوني المسمى نموذج ألوان إشارات المرور (أخضر - أصفر - أحمر) لتمثيل فعالية الضوابط ومستوى المخاطر المتبقية.

وتم استخدام التطبيق سابق الذكر في التقييم اللوني وذلك من خلال الواجهة التالية:

الشكل 16: واجهة تقييم المخاطر وأنظمة الرقابة (ورشات افتراضية) في تطبيق Risk Nucleus

The screenshot shows the 'RCSA - Workshop' interface. The 'Evaluation' window is open, displaying the 'Évaluation finale' section. It features a table with columns for 'Risque inhérent', 'Risque ciblé', and 'Residual Risk'. The table includes rows for 'Impact' and 'Probabilité', with values of 0.000. A 'Justificatif' section is visible, showing a color-coded legend for risk levels: Insignificant (blue), Modéré (yellow), Major (orange), and Catastrophique (red). The interface also includes a sidebar with 'Workshop Details' and a main table with columns for 'VGAC', 'Carte de Chaleur', 'Results', 'Statut', 'Nombre de Contrôles', and 'Nombre de Plans D'action'.

المصدر: تطبيق Risk Nucleus تراست بنك

حيث يساهم هذا النموذج بتصنيف عناصر الخطر وفق درجة خطورتها، مما يسهل على صناع القرار تحديد الأولويات واتخاذ الإجراءات التصحيحية المناسبة (IOR,2010). فعلى سبيل المثال، تم تصنيف خطر استخدام بطاقة مزيفة أو مسروقة على أنه مرتفع (اللون الأحمر نظراً لضعف فعالية نظام التحقق الثنائي (OTP- one time pass-word)، مما استدعى اقتراح تعزيز المصادقة البيومترية.

بينما حُصص اللون الأخضر لمخاطر مثل توقف المنصة التقنية بفضل وجود خطط استمرارية واختبارات دورية فعالة.

أما الخطر المرتبط بتسرب البيانات الحساسة للعملاء فقد اعتُبر من أشد المخاطر (اللون الأحمر)، نظراً لضعف الإجراءات الرقابية، ما تطلّب التوصية بتنفيذ نظام منع تسرب البيانات (DLP) وتدقيق صلاحيات الوصول. وبالمقابل، تم التعامل مع مخاطر الامتثال وتأخر اكتشاف الاحتيال كخطر

متوسط (اللون البرتقالي) نتيجة فعالية جزئية للضوابط القائمة، ما دفع إلى اقتراح تحديث السياسات أو دمج أدوات ذكاء اصطناعي للمراقبة.

هذا النموذج التفاعلي القائم على التصنيف اللوني لا يكفي بعرض مستوى الخطورة فحسب، بل يدعم التقييم الذاتي الجماعي خلال الورشات أو الاستبيانات، ويُعدّ من الأدوات المعترف بها في الأطر التنظيمية الحديثة مثل Basel II و COSO و ISO 31000 (Bessis, 2015؛ Bellini, 2016) كما أنه يسهل التكامل مع مؤشرات المخاطر الرئيسية (KRIs) وخطط العمل التصحيحية، ويُعتبر مناسباً للغاية في بيئات عالية الحساسية كالقطاع المصرفي.

2. أساليب جمع البيانات

يتم اعتماد على أساليب نوعية تشاركية لجمع البيانات مما يتماشى مع طبيعة منهجية التقييم الذاتي للمخاطر والرقابة (RCSA)، التي تقوم على إشراك المعنيين المباشرين في العمليات التشغيلية لتحديد وتقييم المخاطر والضوابط المرتبطة بها ويمكن ومن بين هذه الأساليب:

1.2. أسلوب ورش العمل (Workshop Approach):

يُعد هذا الأسلوب تفاعلياً ويُستخدم لتحفيز النقاش المفتوح بين الموظفين حول المخاطر والضوابط وخطط التحسين.

يُخطط مسبقاً له ويشمل تحديد المشاركين، الأهداف، والموضوعات، كما يجب أن تشمل الورشة ممثلين من كافة الأقسام المعنية لتحقيق تقييم شامل.

عادةً ما يُقسم هذا الأسلوب إلى ثلاث مراحل أساسية: تحديد المخاطر، تحديد وتقييم الضوابط، ثم وضع خطط العمل والمسؤوليات.

يُنصح بجمع البيانات باستخدام شاشة عرض (Data Show) مباشرة لعرض النتائج أمام المشاركين مما يسهل التأكيد الفوري على دقة التوثيق، (IOR, 2010).

2.2. أسلوب الاستبيانات: (Questionnaire Approach): (IOR, 2010).

يعتمد على توزيع استبيانات معيارية أو مخصصة على الجهات المعنية لتقييم فعالية الرقابة الذاتية. تُصمم هذه الاستبيانات لتغطية المخاطر التشغيلية وتقديم معايير قياس مرجعية لتقييم مدى تنفيذ الضوابط.

يمكن أن تكون الأسئلة موحدة (على مستوى المؤسسة) أو مخصصة (حسب القسم)، ويُصحح بأن تكون بصيغة "نعم/لا" مع طلب التفسير في حال الإجابة بـ "لا" أو "غير قابل للتطبيق". تُقيم فعالية التصميم والتنفيذ للضوابط وتُوقع من قبل المستجيبين ثم تُراجع إداريًا لضمان دقة التمثيل.

3.2. الأسلوب الهجين (Hybrid Approach):

يُدمج هذا الأسلوب بين الورش والاستبيانات، حيث تُستخدم ورش العمل في المراحل الأولى لتحديد المخاطر والضوابط، ثم تُستخدم الاستبيانات بشكل دوري لتحديث التقييم أو عند الحاجة. ويُعاد استخدام ورش العمل في حال إدخال أنشطة أو تغييرات جديدة ذات تأثير على المخاطر. هذا الأسلوب يساعد على إبقاء العملية حيوية وفعّالة دون إرهاق المشاركين. (IOR 2010,)

كما يمكن استعان أيضًا بمؤشرات المخاطر الرئيسية (KRIs)، نتائج التدقيق الداخلي، وهو ما يساهم في تحقيق تكامل ثلاثي الأبعاد بين تقييمات الخبراء الميدانيين، المعطيات الكمية المسجلة، والبيانات التاريخية. (Bellini, 2016).

هذا التعدد في الأساليب يساعد على تعزيز مصداقية النتائج من خلال التثليث المنهجي .

مما يعزز صلاحية التقييم ويقلل من التحيزات المرتبطة بالمنهج النوعي القائم على الإدراك الذاتي للمخاطر.

المطلب الثالث: النموذج التطبيقي

1. النموذج التطبيقي:

يجدر الإشارة إلى أننا اعتمدنا أسلوب الورشات دون الاعتماد على الاستبيانات سابقة الذكر وذلك يرجع إلى طبيعة المنهجية المتبع من طرف بنك تراسنت حيث يرتكز هذا النموذج على أسلوب: ورشات العمل التفاعلية، ضمن إطار تحليلي يقوم على ربط المخاطر المحتملة بالأهداف البنك وتحليل فعالية الضوابط الحالية، ومن ثم قياس مستوى المخاطر المتبقية (Residual Risk) وفقاً لمصفوفات تقييم.

كما يعتمد هذا النموذج على تصنيف المخاطر إلى مخاطر كامنة (Inherent Risks) ومخاطر متبقية بعد تطبيق الضوابط، إضافة إلى تقييم فعالية تصميم وتنفيذ الرقابة باستخدام أدوات مثل خرائط

الحرارة (Heat Maps) (الشكل 18) وخطط المعالجة (Action Plans) (الشكل 17)

الشكل 17: مضمون مخططات العمل في تطبيق Risk Nucleus

Résumé du plan

ID du plan d'action	AP001267	Statut	Clôturé
Intitulé du plan d'action	Edition pièce comptable avances administratives		
Action Plan Department	Direction Informatique et Techn		
Directeur d'entité	[Redacted]	Action attribuée à	[Redacted]
Type de plan d'action	Correctif	Type de résolution	Solution permanente
Date de début	01 Jun 20	Date prévue de finalisation	31 Jan 20
Date de finalisation effective	05 Mar 20	Gravité	Normal
Coût associé au plan d'action	<input type="checkbox"/>		
Description du plan d'action	Lors du débloccage des avances administratives, les pièces comptables ne s'éditent pas. Investigation en cours		

Liens plan

Incident lié	Edition pièce comptable (EVT00474)	[Icon]
IC lié	[Redacted]	[Icon]
Risque lié	[Redacted]	[Icon]

المصدر: تطبيق Risk Nucleus تراست بنك

يعرض الشكل 17 نموذجًا من نظام إدارة المخاطر يتضمن بطاقة خطة عمل تصحيحية تم تنفيذها من طرف قسم Direction Informatique et Technologies بالبنك تحتوي البطاقة على معلومات أساسية مثل معرف الخطة، نوع الإجراء (تصحيحي)، وتواريخ التنفيذ الفعلي والمتوقع، إضافة إلى وصف موجز للمشكل المرتبط بعدم إمكانية تحرير القطع المحاسبية عند صرف التسبيقات الإدارية. كما توضح البطاقة أن الإجراء المتخذ يندرج ضمن "حل دائم" مع تصنيف درجة الخطورة على أنها "عادية". في الأسفل، تُعرض الروابط المرتبطة بالخطة مثل الحادث الأصلي والخطر المتعلق به، مما يُبرز الترابط بين مختلف مكونات النظام ويُسهل تتبع تنفيذ الإجراءات التصحيحية بشكل فعال أما بالنسبة للشكل الموالي رقم 18 فهو يمثل النتيجة النهائية لورشات العمل والذي سوف نشرحه في الفقرة الموالية

الشكل 18: نتائج ورشة تقييم المخاطر الخامة والصادفة في تطبيق Risk Nucleus



المصدر: تطبيق Risk Nucleus تراست بنك

تمثل الخريطة الحرارية للمخاطر (Heat Map) أداة تحليلية مهمة تُستخدم لتقييم مستوى المخاطر داخل المؤسسات، من خلال تصنيفها بناءً على مدى احتمالية حدوثها (Likelihood) وتأثيرها المحتمل (Impact) ويُظهر المثال المرفق مصفوفتين للمخاطر: الأولى تمثل المخاطر الكامنة (Inherent Risk)، وهي تلك المخاطر قبل تطبيق أية تدابير رقابية، والثانية تمثل المخاطر المتبقية (Residual Risk) بعد تنفيذ الضوابط والإجراءات الرقابية. تُعرض المخاطر وفق شبكة تجمع بين أربعة مستويات لاحتمالية الحدوث (من "نادر" إلى "متكرر") وأربعة مستويات للأثر المالي (من "ضئيل" إلى "كارثي")، مما ينتج خلايا ملونة تعكس درجة الخطورة، حيث يشير اللون الأخضر إلى مخاطر منخفضة، والأصفر إلى متوسطة، والبرتقالي إلى مرتفعة، والأحمر إلى مخاطر حرجة. يُلاحظ من خلال هذا المثال أن بعض المخاطر التي كانت مصنفة ضمن مستوى خطر مرتفع أو حرج في المصفوفة الكامنة، قد تم تخفيضها إلى مستويات أقل في المصفوفة المتبقية، ما يعكس فعالية التدابير المتخذة في تقليص شدة الخطر واحتمالية وقوعه.

2. طريقة الحساب المعتمد من طرف Risk Nucleus:

يعتمد تطبيق Risk Nucleus في تقييم المخاطر التشغيلية على ثلاث طرق حسابية رئيسية، هي: المتوسط (Mean)، الذي يُستخدم لحساب القيمة الوسطية بين درجة الاحتمالية والتأثير ويعكس توازن الخطر، والمنوال (Mode)، الذي يُعتمد لتحديد الدرجة الأكثر تكرارًا بين عدة تقييمات، مما يعبر عن الرأي الغالب أو الإجماع. تتيح هذه الطرق مرونة في التقدير، وتُستخدم بحسب طبيعة البيانات المتوفرة وأهداف التحليل.

في بنك تراست، يتم اعتماد طريقة المنوال في التقييم، حيث يُمنح كل مشارك وزن (نقل) محدد في عملية التصويت، بما يضمن مراعاة أهمية كل رأي في التقدير النهائي. وسيتم توضيح آلية هذا التقييم بشكل أكثر تفصيلاً في الشكل التوضيحي الموالي.

الشكل 19: واجهة دمج نتائج ورشات تقييم المخاطر في تطبيق Risk Nucleus

The screenshot displays the 'RCSA - Workshop' interface. A 'Confirmation' dialog box is open, asking the user to select the method of voting consolidation. The options are 'Weighted Average' (selected) and 'Mode (Most Repeated)'. The background interface shows a table of risks with columns for ID, Description, Evaluation, TA, Evaluation résiduelle, VGAC, Carte de Chaleur, and Results. Two risk entries are visible: RSK353 and RSK5415. The interface also includes navigation buttons at the top and a summary section at the bottom.

المصدر: تطبيق Risk Nucleus تراست بنك

الفصل الثالث: تحليل النتائج و المناقشة

يُعد الجانب التطبيقي من هذا البحث محطة محورية لترجمة الأطر النظرية والمنهجيات المعتمدة إلى واقع عملي يعكس الخصوصيات التشغيلية للمؤسسة البنكية وفي هذا الإطار تم التركيز على إعداد خارطة مخاطر خاصة ببطاقة الدفع البنكية، باعتبارها من أكثر المنتجات البنكية عرضة للمخاطر التشغيلية نتيجة لتعدد الجهات الفاعلة وتشابك العمليات، وتزايد الاعتماد على الأنظمة الرقمية في بيئة مصرفية ديناميكية.

ويهدف هذا الجانب إلى تحليل النشاط الفعلي المرتبط ببطاقة الدفع من خلال نمذجة تفصيلية لمراحله المختلفة (طلب البطاقة، التفعيل، الاستخدام، والتسوية)، تمهيداً لتحديد المخاطر المرتبطة بكل مرحلة ولضمان موثوقية النتائج، تم اعتماد على منهجية RCSA - Risk and Control Self-Assessment (Assessment) شملت ورشات عمل مع مسؤولين من البنك، تحليل وثائقي للإجراءات والنظم الداخلية، وملاحظة ميدانية مباشرة لسير العمليات كما تم توظيف أدوات وتقنيات حديثة مثل خريطة المخاطر (Risk Mapping)، وجداول تقييم المخاطر المبنية على معايير دولية (ISO, COSO ERM)، و(PCI DSS)، وذلك لتكوين تصور شامل ومتكامل لمواطن الضعف والسيطرة المرتبطة باستخدام بطاقات الدفع البنكية.

المبحث الأول : تحليل العمليات وتحديد المخاطر في بطاقة الدفع

1. المفاهيم الأساسية في الجانب التطبيقي:

1.1. نمذجة الأنشطة (Modélisation des activités): هي عملية تحليلية ومنهجية تهدف إلى تمثيل الأنشطة التنظيمية بشكل مرئي أو وصفي، لتحديد الأهداف التشغيلية، والضوابط القائمة لضمان تحقيق هذه الأهداف. وتُعد هذه النمذجة خطوة أولية أساسية في إطار تقييم المخاطر التشغيلية، حيث تساهم في فهم النشاطات داخل المؤسسة. (I O R, 2010).

تتقسم نشاطات تراست بنك إلى أربع عائلات:

- النشاط التجاري
- النشاطات الداعمة
- نشاطات الرقابة
- النافذة الإسلامية

2.1. تحديد الميغا-عمليات (Identification des Mega-processus) :

يُعد تحديد "الميغا-عمليات" خطوة محورية في بناء إطار منظم لتقييم المخاطر التشغيلية المرتبطة ببطاقات الدفع البنكية، حيث يسمح هذا التمرين بتقسيم النشاطات إلى وحدات كبرى مترابطة تُشكّل الأساس لتحليل المخاطر والضوابط المرتبطة بها ويُعرّف الميغا-بروسيس (Mega-processus) على أنه سلسلة مترابطة من العمليات الكبرى التي تنظم تدفق الأنشطة وتدعم تحقيق أهدافها التشغيلية والرقابية (I O R, 2010).

مثلا: إذا قمنا بتجزئة النشاطات الداعمة إلى ميغا - عمليات نجد ما يلي:

- تسيير الموارد البشرية
 - تسيير أنظمة المعلومات
 - تسيير المباني والمنشأة
 - تسيير وسائل الدفع (الذي يحتوي بداخله على عمليات تسيير بطاقات الدفع موضوع بحثنا هذا)
- إلى أخيره

3.1. تحديد عمليات (Identification des processus)

في هذا السياق، يساهم هذا التحديد في تمكين البنك من اعتماد مقارنة تقييم المخاطر على أساس "من البداية إلى النهاية (End-to-End)"، كما يُوصى به في إطار التقييم الذاتي لمخاطر والرقابة (RCSA)، ما يسمح بتحليل شامل للعمليات المرتبطة ببطاقات الدفع، بدءًا من طلب البطاقة، مرورًا بإنتاجها وتفعيلها، وصولاً إلى استخدامها والتسوية والتقارير المتعلقة بها. هذا الأسلوب يسهل أيضًا الكشف عن الثغرات الرقابية، وتحديد المكونات المعرضة للخطر، وتوجيه الجهود نحو التحسين المستمر للضوابط. (I O R, 2010).

4.1. جرد العمليات (Inventaire des processus):

يُعد جرد العمليات خطوة أساسية ومكملة لتحديد الميغا-عمليات، حيث يتم من خلالها حصر وتصنيف العمليات الفرعية التي تتدرج ضمن كل ميغا-عملية بشكل دقيق ومنهجي. ويسمح هذا الجرد بإعداد خريطة تفصيلية لتسلسل المهام، الجهات المتدخلة، والمخرجات المتوقعة، ما يُسهم في تعزيز الفهم الشامل للنشاط وتحديد نقاط الخلل المحتملة التي قد تشكل مصدرًا للمخاطر التشغيلية (I O R, 2010). في إطار ممارسة التقييم الذاتي لمخاطر الرقابة (RCSA)، يوصي معهد المخاطر التشغيلية بجرد العمليات كخطوة أولى لتحديد الأهداف، المخاطر، والضوابط المرتبطة بها، وذلك لضمان شمولية التقييم وتماسكه عبر جميع وحدات العمل (IOR,2010) ويُعد هذا التمرين ضروريًا لتحديد أماكن وجود الضوابط، تقييم فعاليتها، ومعرفة ما إذا كانت متناسبة مع طبيعة المخاطر في كل مرحلة من مراحل دورة حياة بطاقة الدفع البنكية. (I O R, 2010).

في حالة دراستنا اخترنا العمليات المتعلقة بتسيير بطاقات الدفع البنكية والتي بذاتها تنقسم إلى عدة عمليات ومنها:

- شراء البطاقات فارغة (غير مشخصة)
- تسيير مخزون البطاقات الفارغة
- شخصنة البطاقات عند الطلب
- توزيع البطاقات على الوكالات
- تسيير المخزون على مستوى الوكالات
- تسليم البطاقات للزبائن
- تفعيل البطاقة
- معالجة طلبات وشكاوى الزبائن

2. خارطة المخاطر التشغيلية المتعلقة ببطاقة الدفع البنكية (CIB):

1.2. عرض المنهجية المعتمدة

- تعتمد منهجية إعداد خارطة المخاطر التشغيلية المرتبطة بإدارة بطاقات الدفع البنكية على مجموعة من التحضيرات الأساسية التي تهدف إلى ضمان دقة وشمولية التحليل. وتتمثل هذه التحضيرات فيما يلي:
- جمع الوثائق المرجعية الخاصة ببطاقة الدفع البنكية، والتي تشمل الإجراءات التشغيلية المعتمدة، البطاقة التقنية للمنتج، بطاقات المراقبة، إلى جانب الهيكل التنظيمي للإدارة المسؤولة عن التسيير؛
 - مراجعة خارطة المخاطر السابقة، إن وُجدت، وتحليل مؤشرات المخاطر الرئيسية (KRI)، إضافة إلى استخراج وتحليل بيانات الحوادث التشغيلية المسجلة والمتعلقة باستخدام هذا المنتج البنكي؛

- تحديد الأطراف المعنية بالعملية، سواء كانوا فاعلين مباشرين أو غير مباشرين، مع توضيح مهامهم وأدوارهم ضمن سلسلة تسيير بطاقات CIB، وذلك قصد إشراكهم لاحقاً في ورشات العمل الخاصة بإعداد خارطة المخاطر، لما في ذلك من فائدة في إثراء التحليل وضمان واقعيته.

- تحديد الوسائل المادية والمعلوماتية اللازمة لتسيير بطاقة الدفع CIB

تمثل هذه الخطوات التمهيدية الأساس المنهجي لإنجاز خارطة مخاطر دقيقة، تعكس البيئة التشغيلية الحقيقية وتُسهم في تحسين فعالية الرقابة وإدارة المخاطر ذات الصلة ببطاقات الدفع البنكية.

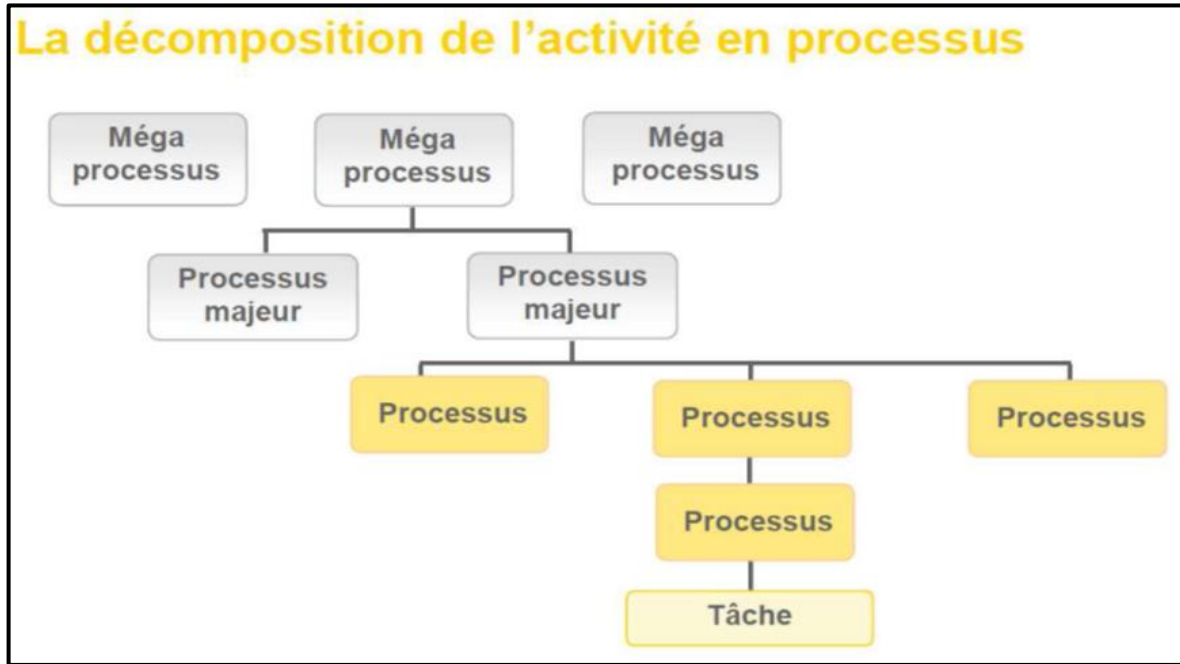
2.2. تجزئة للعمليات التشغيلية: (I O R, 2010)

تُعد مرحلة تفكيك العملية الرئيسية إلى عمليات فرعية خطوة منهجية أساسية في نمذجة العمليات ضمن سياق إدارة المخاطر التشغيلية في هذه المرحلة، يتم تقسيم كل "ميغا-عملية" إلى سلسلة من العمليات الفرعية المترابطة، والتي بدورها تُحلل إلى مهام ووحدات عمل دقيقة، مما يسمح بفهم أكثر لتسلسل العمليات وتحديد نقاط الضعف المحتملة داخل كل مستوى (الشكل 20)

هذا النهج يتيح للمؤسسة:

- التعرف بدقة على مسارات تدفق العمل.
- تحديد المهام الحرجة التي قد تكون مصدرًا للمخاطر.
- تعيين المسؤوليات بشكل واضح عبر جميع مستويات النشاط.
- تسهيل رسم خارطة المخاطر وربطها بمهام فعلية يمكن مراقبتها وتحسينها

الشكل 20: تجزئة النشاطات والعمليات التشغيلية



المصدر: [Document de travail, Trust Bank Algérie].

3. مرحلة التوثيق وفهم العمليات في بطاقة الدفع:

يعرض الجدول رقم 8 تقسيمًا دقيقًا للعملية الكاملة الخاصة بقسم بطاقات الدفع (الوطنية والدولية)، بدءًا من اقتناء البطاقات، وتخصيصها، إلى تسليمها للعملاء، ثم التعامل مع حالات الحظر المؤقت أو الدائم، وصولًا إلى معالجة الاعتراضات سواء على المستوى الوطني أو الدولي. لكل عملية رئيسية، يتم تصنيف العمليات الفرعية والمهام المحددة ضمن سلسلة الإجراءات المتبعة، مع بيان ما إذا كانت تُنفذ داخليًا أو بالاستعانة بمزود خدمة خارجي. كما يساهم الجدول في إبراز نقاط التداخل بين مختلف المصالح المعنية، ويساعد على تحديد المسؤوليات بدقة.

يُعد هذا التصنيف أساسًا مهمًا لتقييم المخاطر التشغيلية بدقة، ويساعد في بناء خارطة مفصلة تسهّل عملية التحليل والمراقبة المستمرة للعمليات.

الجدول رقم 8: مرحلة التوثيق وفهم العمليات لبطاقة الدفع البنكية في بنك تراست

Volet couvert par une procédure (Oui/Non/Réf)	Processus	Sous Processus	sous processus	Taches
Oui	Gestion des cartes de paiements (nationale / Internationale)	Acquisition des cartes	Commande d'un lot de carte vierges (CIB, VISA et Mastercard)	Gestion de la relation et du compte clients
				Gestion de la relation et du compte clients
			Réception et vérification du lot reçu (CIB et VISA stocké à la	Gestion de la relation et du compte clients
			Envoi des Mastercard et des codes aux agences (et suivi du stock détenu)	Gestion de la relation et du compte clients
		Personnalisation des cartes (CIB et VISA)	Validation des octrois de cartes faites par les agences (A travers la comptabilisation sur Banks des commissions)	Gestion de la relation et du compte clients
			Transmission au quotidien des fichier (CIB à personnaliser) à SATIM sur le portail	Gestion de la relation et du compte clients
			Transmission hebdomadaire des fichier (ViSA à personnaliser) à partir FTP	Gestion de la relation et du compte clients
		Octroi des cartes aux clients (Acquisition et renouvellement)	Réception des cartes personnalisées et codes séparation (SATIM, DHL et FedEx)	Gestion de la relation et du compte clients
			Vérification du lot et envoi des cartes et codes aux agences	Gestion de la relation et du compte clients
			Pour la Mastercard transmission du fichier des rechargement	Gestion de la relation et du compte clients
			pour activation	Gestion de la relation et du compte clients
				Gestion de la relation et du compte clients
		Blocage Temporaire ou définitif, Déblocage et Résiliation	Réception d'une demande de blocage, déblocage ou de résiliation de carte sur TrustCard	Gestion de la relation et du compte clients
			Génération du fichier des mises à jour	Gestion de la relation et du compte clients
			Transmission du fichier au processeur pour exécution	Gestion de la relation et du compte clients
		Gestion des litiges cartes nationales	Génération automatique du fichier des réclamations sur cartes CIB à partir de TRUST CARD	Gestion de la relation et du compte clients
		Gestion des litiges cartes Internationales	Vérification du charge Back signé par le client et transmission à EMP pour cartes internationales	Gestion de la relation et du compte clients
			Informé l'agence du résultat d'analyse de EMP et suivi de la résolution des réclamations sur cartes	Gestion de la relation et du compte clients

المصدر: من إعدادنا بتطبيق RISK NUCLEUS

عندما يتم توثيق وفهم العمليات لبطاقة الدفع البنكية ننتقل إلى تحديد وتصنيف وتقييم المخاطر

المرتبطة بكل عملية

المبحث الثاني : تقييم وتحديد وتصنيف المخاطر

1. تحديد المخاطر:

في هذه المرحلة، يقوم المشاركون في ورشات العمل، وهم في الغالب الأشخاص الذين يزاولون المهام فعلياً على أرض الواقع، بوصف دقيق لكل مهمة من المهام المندرجة ضمن العملية قيد الدراسة. ومن خلال هذا الوصف العملي، يتم السعي إلى تحديد المخاطر المحتملة التي قد تنشأ أثناء تنفيذ كل مهمة، والتي تُعرف بـ المخاطر المتأصلة (risques inhérents) أي بدون أخذ بعين الاعتبار وجود نظام رقابي.

عند تحديد كل خطر، وبعد موافقة جميع الحضور يُطلب من المشاركين تقديم عنوان مختصر لهذا الخطر، بالإضافة إلى وصف واضح لطبيعته وأسباب وقوعه وتأثيره

الجدول رقم 9: المخاطر الخاصة ببطاقة الدفع البنكية

Processus (4)	S/Processus (9)	Volet couvert par une procédure	Nombre de risque (34)
Organisation	Constitution de la journée comptable		3
Transaction Monétique	Retrait et Paiement (DAB TPE)	Oui	2
Gestion des cartes de paiements (nationale / Internationale)	Personnalisation des cartes (CIB et VISA)	Oui	7
	Octroi des cartes aux clients (Acquisition et renouvellement)	Oui	6
	Blocage Temporaire ou définitif, Déblocage et Résiliation	Oui	3
	Gestion des litiges cartes internationales	Oui	2
	Gestion des litiges cartes nationales	Oui	1
Gestion des moyens de paiements (TPE, DAB)	TPE	Oui	5
	DAB	Oui	5

المصدر: من إعدادنا بتطبيق Risk Nucleus

يعرض الجدول رقم 9 هيكلًا تفصيليًا للعمليات الأساسية والفرعية

(Processus / Sous-Processus) المتعلقة بإدارة بطاقات الدفع والمعاملات النقدية داخل بنك تراست

ويشمل أربع عمليات رئيسية تغطي الجوانب التنظيمية، والمعاملات النقدية، وإدارة بطاقات الدفع (الوطنية

والدولية) ، بالإضافة إلى إدارة وسائل الدفع لكل عملية فرعية يُبين الجدول ما إذا كانت مغطاة بإجراء

مكتوب

كما يعرض عدد المخاطر التشغيلية التي تم تحديدها في كل منه (Nombre de Risque)

يُلاحظ أن عملية تخصيص البطاقات CIB و VISA تسجل أعلى عدد من المخاطر

(7 مخاطر)، ما يشير إلى حساسية هذه المرحلة وأهميتها في منظومة الدفع.

الجدول يمثل أداة تشخيصية أولية لرسم خارطة المخاطر التشغيلية المرتبطة بدورة حياة بطاقات الدفع

البنكية، ويمكن استخدامه كأساس لتطوير خطة تقييم وتحسين الضوابط الداخلية.

2. تصنيف المخاطر:

بعد ذلك، يتم تصنيف كل خطر ضمن إحدى الفئات السبع المعتمدة من طرف لجنة بازل، وهي تصنيفات

معيارية تُستخدم على نطاق واسع لتوحيد فهم وتقييم المخاطر التشغيلية داخل المؤسسات البنكية والمالية.

تُعرض هذه الفئات السبع للمخاطر بشكل مفصل في الملحق رقم 1، وتشمل على سبيل المثال مخاطر

داخلية ناتجة عن الأخطاء البشرية، أو فشل الأنظمة، أو تلك المرتبطة بعمليات احتيال داخلية أو

خارجية.

يمثل الشكلان الموضحان في الشكل رقم 22 تحليلًا تصنيفيًا للمخاطر التشغيلية المرتبطة ببطاقات الدفع

البنكية وذلك من خلال منظورين مختلفين:

1.2. تصنيف حسب السبب: (Classification par cause)

يعرض هذا الرسم توزيع المخاطر حسب مصدرها أو العامل المسبب لها:

تأتي العمليات (Process) في الصدارة بـ 14 مخاطرة، ما يعكس أهمية كفاءة الإجراءات وجودة سير العمل.

يليه العامل البشري (People) بـ 10 مخاطر، مما يشير إلى أهمية التكوين والرقابة على الموظفين.

بينما تُسجل المخاطر النظامية (System) والخارجية 5 (External) لكل منهما ما يدل على أهمية البنية التحتية الرقمية والتفاعل مع العوامل البيئية الخارجية.

2.2. تصنيف حسب فئة المخاطر:

يُظهر هذا الرسم تصنيف المخاطر التشغيلية وفقًا لإطار التصنيف المستخدم غالبًا في المعايير الدولية مثل: إطار بازل II

تهيمن فئة التنفيذ والتسليم وإدارة العمليات (Execution, delivery & process management) بـ 27 حالة، مما يؤكد التركيز على خلل أو ضعف في العمليات الداخلية.

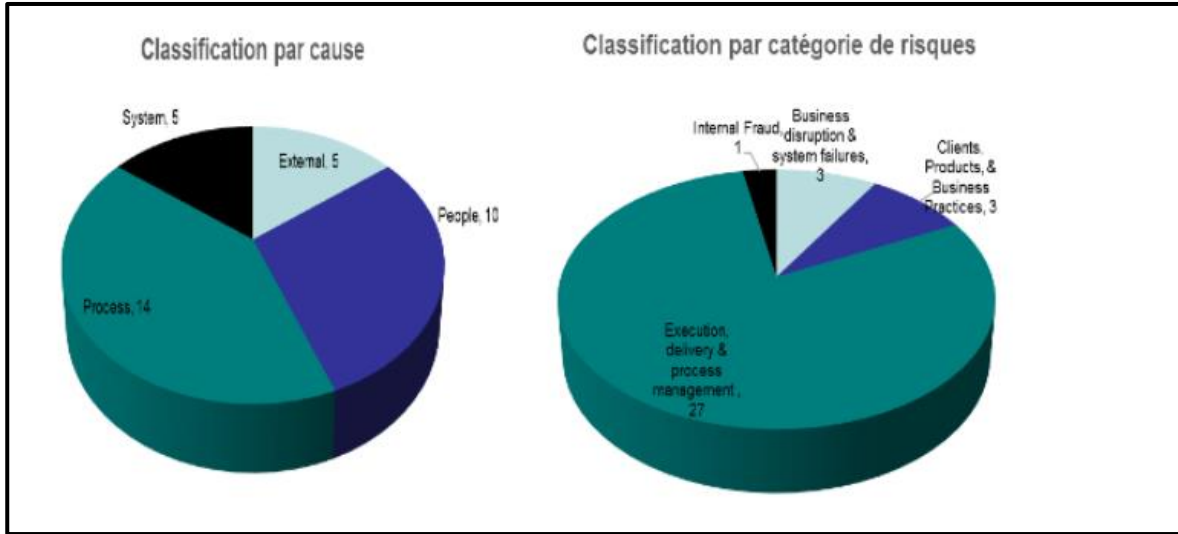
تليها فئتا العملاء والمنتجات والممارسات التجارية (3 حالات) والاضطرابات التقنية/فشل الأنظمة

(3 حالات) وهو ما يسلط الضوء على بعض التحديات ذات الطابع التقني أو المرتبطة بخدمة الزبائن.

بينما تُسجل الاحتيالات الداخلية (Internal Fraud) أقل عدد بمخاطرة واحدة فقط ما قد يعكس

فعالية الرقابة في هذا الجانب أو ضعف في رصد هذا النوع من المخاطر

الشكل رقم 22: تحديد وتصنيف المخاطر



المصدر: من إعدادنا بتطبيق Risk Nucleus

3. تقييم المخاطر:

تقييم المخاطر في بطاقة الدفع البنكية يشير إلى عملية تحليل وتحديد المخاطر التي قد تواجه المستخدمين أو البنك أثناء استخدام بطاقات الدفع مثل بطاقات الائتمان أو الخصم. تشمل هذه المخاطر عدة جوانب، مثل الاحتيال، السرقة، الاستخدام غير المصرح به، أو الهجمات الإلكترونية على أنظمة الدفع.

تهدف هذه العملية إلى تحديد الثغرات الأمنية المحتملة وتطوير استراتيجيات لتقليل هذه المخاطر قد يتضمن ذلك تطبيق تقنيات أمان مثل التشفير، التحقق متعدد العوامل، والمراقبة المستمرة للمعاملات للكشف عن أي نشاط غير عادي. الهدف النهائي هو حماية بيانات المستخدم وضمان سلامة المعاملات المالية.

المشاركون في الورشات يقومون بتقييم المخاطر حسب العاملين:

- احتمالية تكرار وقوع الحادث (probability)

- التأثير المالي لكل حادثة (impact)

وهذا التقييم يكون بالاستعانة بمصفوفة تقييم المخاطر الخاصة بالبنك (RAM- Risk assessment)

matrix كما يوضحها الشكل رقم 23

الشكل 23: مصفوفة تقييم المخاطر في بنك تراست (تم تعديل الأرقام لأغراض متعلقة)

	MAJEUR (100K à 500K)	Moyen	High	Elevé	Elevé
	IMPORTANT (50K à 100K)	Moyen	Elevé	Elevé	Elevé
	MOYEN(10K à 50K)	Bas	Moyen	Moyen	Elevé
	MINIME(1000 à 10K)	Bas	Bas	Moyen	Moyen
		RARE (once in 2-5 years)	IMPROBABLE (once in 1-2 years)	MOYEN (1 to 3 times a year)	PROBABLE (4 to 11 times a year)
	PROBABILITE				

المصدر: من إعدادنا بتطبيق Risk Nucleus

4. نتائج التقييم الذاتي للمخاطر والرقابة:

يعرض الشكل رقم 24 تحليلاً مقارناً لمستوى المخاطر داخل بنك قبل وبعد تطبيق الضوابط الرقابية.

الجزء الأيسر يمثل المخاطر الكامنة (Risque Inhérent) أي المخاطر التي قد يواجهها البنك في حال عدم وجود أي ضوابط أو إجراءات تحكم، حيث يُلاحظ وجود 28 خطراً عالياً و6 مخاطر متوسطة أما الجزء الأيمن فيعرض المخاطر المتبقية (Risque Résiduel) بعد تطبيق الضوابط حيث تتخفف المخاطر العالية بشكل ملحوظ إلى حالتين فقط مقابل ارتفاع عدد المخاطر المنخفضة إلى 20 حالة.

الشكل رقم 24: نتائج التقييم الذاتي للمخاطر والرقابة



المصدر: من إعدادنا بتطبيق Risk Nucleus

تشير هذه النتائج إلى أن 75% من الضوابط المعتمدة كانت فعالة في تقليص شدة المخاطر، مما يُعد مؤشراً إيجابياً على كفاءة منظومة التحكم الداخلي في المؤسسة محل الدراسة.

5. نتائج التقييم الذاتي للمخاطر والرقابة حسب كل عملية:

يمثل الشكل 25 تحليلاً كمياً لمستوى المخاطر التشغيلية المرتبطة بالعمليات الفرعية الخاصة ببطاقات

الدفع من خلال مقارنة بين المخاطر الجوهرية (Score Inhérent) والمخاطر المتبقية

(Score Résiduel) عبر 9 عمليات فرعية. من حيث المخاطر الجوهرية تُظهر النتائج أن 6 عمليات

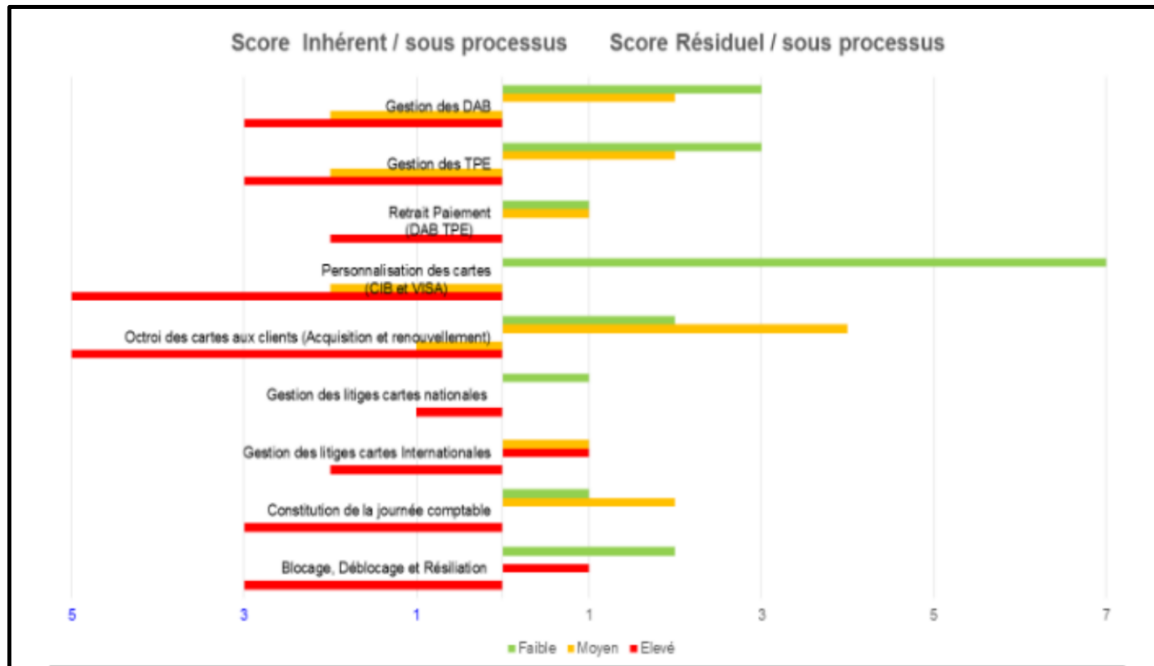
(أي ما يمثل 66.66%) تصنف ضمن فئة المخاطر المرتفعة في حين أن عمليتين (22.22%) في

مستوى متوسط وعملية واحدة فقط (11.11%) في مستوى منخفض.

بالمقابل بعد تطبيق إجراءات الرقابة تم تسجيل انخفاض ملحوظ في مستوى الخطر حيث أن 5 عمليات (55.55%) أصبحت في مستوى منخفض 4 عمليات فقط (44.44%) بقيت في مستوى متوسط مع عدم تسجيل أي عملية في مستوى خطر مرتفع.

تبرز عملية منح البطاقات للعملاء (الاكتساب والتجديد) كأعلى العمليات خطورة من حيث الخطر الجوهري إذ أنها تسجل مستوى مرتفع جدًا وتبقى حتى بعد الرقابة في مستوى متوسط مما يدل على ضرورة تعزيز التدابير الوقائية والرقابية في هذه النقطة الحساسة تعكس هذه النتائج بوضوح فعالية نظام الرقابة المعتمد حيث تمكن من خفض الخطر في معظم العمليات مما يساهم في تحسين الأمن التشغيلي وتقليل احتمالات وقوع حوادث تشغيلية مؤثرة في نشاط البطاقات.

الشكل 25: نتائج التقييم الذاتي للمخاطر والرقابة حسب كل عملية فرعية / عملية تشغيلية



المصدر: من إعدادنا بتطبيق Risk Nucleus

يعرض الجدول رقم 10 تحليلاً كمياً مفصلاً لمستويات المخاطر الجوهرية والمخاطر المتبقية المرتبطة بتسعة عمليات فرعية خاصة بنظام بطاقات الدفع، وفقاً لتقييم ثلاثي المستويات (مرتفع، متوسط،

منخفض) فيما يتعلق بالمخاطر الجوهرية (Scoring Inhérent) يُلاحظ أن 7 من أصل 9 عمليات (أي بنسبة 78%) تصنّف ضمن فئة المخاطر المرتفعة في حين أن عمليتين فقط (22%) تقعان في المستوى المتوسط دون تسجيل أي مستوى منخفض هذا يدل على أن أغلب العمليات تنطوي على مخاطر جوهرية مرتفعة بطبيعتها قبل تطبيق أي إجراءات رقابية.

أما فيما يخص المخاطر المتبقية (Scoring Résiduel) فتُظهر النتائج تحسّناً واضحاً بعد تطبيق آليات الرقابة حيث تم تخفيض نسبة المخاطر المرتفعة إلى 2 من أصل 9 عمليات فقط (22%) في حين أصبحت 3 عمليات (33%) في مستوى متوسط و4 عمليات (44%) في مستوى منخفض على سبيل المثال تم تقليص مستوى الخطر في عملية إدارة النزاعات الوطنية من 100% خطر جوهرى مرتفع إلى 100% خطر متبقي منخفض، وهو ما يعكس فعالية عالية للرقابة في هذه الحالة في المقابل تبقى عملية منح البطاقات للعملاء بحاجة إلى مراجعة أعمق إذ تسجل 83% خطر جوهرى مرتفع ولا تزال تحتفظ بنسبة 67% من الخطر في المستوى المتوسط بعد الرقابة.

بشكل عام يُظهر هذا التحليل أن البنك يعتمد على آليات رقابة فعالة نسبياً تمكنت من خفض مستوى المخاطر المتبقية في عدد من العمليات إلا أن بعض النقاط، مثل عمليات الإيقاف/إلغاء البطاقات أو منحها، ما تزال تستوجب تعزيز التدخلات الرقابية لتقليل درجة التعرض للخطر بشكل أكبر.

الجدول 10: نتائج التقييم الذاتي للمخاطر والرقابة حسب كل عملية فرعية / عملية تشغيلية

S/Processus	Scoring Inhérent		Scoring Résiduel		
	Elevé	Moyen	Elevé	Moyen	Faible
Blocage, Déblocage et Résiliation	100%	0%	33%	0%	67%
Constitution de la journée comptable	100%	0%	0%	67%	33%
Gestion des litiges cartes Internationales	100%	0%	50%	50%	0%
Gestion des litiges cartes nationales	100%	0%	0%	0%	100%
Octroi des cartes aux clients (Acquisition et renouvellement)	83%	17%	0%	67%	33%
Personnalisation des cartes (CIB et VISA)	71%	29%	0%	0%	100%
Comptabilisation des transactions monétique (DAB TPE)	100%	0%	0%	50%	50%
Gestion des TPE	60%	40%	0%	40%	60%
Gestion des DAB	60%	40%	0%	40%	60%

المصدر: من إعدادنا باستعانة بتطبيق Risk Nucleus

6. تفاصيل في عمليتين أساسيتين في المخاطر التشغيلية المرتبطة ببطاقة الدفع البنكية:

يعرض الجدول 11 تحليلاً نوعياً وكمياً للمخاطر التشغيلية المرتبطة بعمليتين فرعيتين أساسيتين ضمن عملية إدارة بطاقات الدفع (الوطنية والدولية) وهما منح البطاقات للعملاء (الاكتساب والتجديد) وإدارة النزاعات الخاصة بالبطاقات الدولية تم تقييم خمسة مخاطر تشغيلية حيث صُنِّفت أربعة منها (أي بنسبة 80%) كمخاطر جوهرية مرتفعة بينما صُنِّف خطر واحد فقط (20%) كخطر جوهري متوسط وبعد تطبيق إجراءات الرقابة تم تخفيض جميع هذه المخاطر إلى مستوى متبقٍ متوسط، بنسبة 100% دون تسجيل أي خطر منخفض أو مرتفع وتعلق أبرز المخاطر المرتبطة بعملية منح البطاقات بمشكلات مثل إعادة شحن البطاقة مرتين أو تأخر إرسال ملفات تفعيل بطاقات Mastercard، إضافة إلى التحقق غير الكافي من ملفات شحن Hissabi، وكلها مصنفة كمخاطر مرتفعة في حال غياب الرقابة كما تم

رصد خطر مرتبط بعملية إدارة النزاعات الدولية يتمثل في تنفيذ عمليات في وضع غير متصل وهو ما يحمل احتمالاً كبيراً لعدم التسديد وقد ساهمت الرقابة المعتمدة مثل المراقبة اليومية، والمطابقة بين الأنظمة، والتحقق اليدوي، في تقليص هذه المخاطر إلى المستوى المتوسط وبالرغم من هذا التحسن، إلا أن النتائج تُظهر ضرورة تعزيز فعالية الرقابة أكثر من خلال حلول تقنية وتنظيمية إضافية، بهدف تقليص هذه المخاطر إلى مستوى منخفض خاصة في العمليات الحساسة المتعلقة بإعادة الشحن والتفعيل.

الجدول 11: تفاصيل في عمليتين أساسيتين في المخاطر التشغيلية المرتبطة ببطاقة الدفع

Processus	Sous Processus	Intitulé du risques	Score Inhérent	Intitulé du contrôle	Score Résiduel
Gestion des cartes de paiements (nationale / Internationale)	Octroi des cartes aux clients (Acquisition et renouvellement)	Erreur d'acheminement des cartes / codes aux agences	Moyen	Les courriers pour les agences sont préparés par un des collaborateur et vérifiés par un autre	Moyen
		Rechargement d'une carte en double	Elevé	Un rapprochement mensuel est effectué entre le compte trust et EMP si le montant est différent, les opérations sont alors pointées pour détecter l'anomalie	Moyen
		Fichier d'activation des mastercard non transmis ou transmis tardivement	Elevé	Le premier responsable de structure veille à ce que tous les fichiers générés ont bien été transmis aux destinataires concernés	Moyen
		Mauvaise vérification des fichiers Hissabi (rechargement Mastercard)	Elevé	Vérification quotidienne des rechargement Hissabi en cas d'anomalie l'agence est prier de contacter son client pour confirmation ou infirmation de l'opération	Moyen
	Gestion des litiges cartes Internationales	Exécution d'une opération en offline (risque d'impayé)	Elevé	Vérification quotidienne des transactions, en cas d'impayé la carte du client bloquer immédiatement	Moyen

المصدر: من إعدادنا باستعانة بتطبيق Risk Nucleus

المبحث الثالث: مناقشة النتائج و الاقتراحات

1. الأهداف والمنهجية:

الهدف الأساسي: إعداد خارطة مخاطر مفصلة لبطاقات الدفع من خلال نمذجة دورة حياتها (طلب، تفعيل، استخدام، تسوية).

المنهجية المعتمدة: تم اعتماد منهجية RCSA التقييم الذاتي للمخاطر والرقابة وتم تطبيقها من خلال:

- تنظيم ورش عمل تشاركية مع موظفين من مختلف الأقسام.
- إجراء تحليل وثائقي للسياسات والإجراءات.
- ملاحظة ميدانية مباشرة للعمليات.

2. الأدوات والتقنيات:

توظيف تطبيق RISK NUCLEUS لبناء خارطة تفاعلية للمخاطر، يتضمن:

- مصفوفات تقييم (للمخاطر الكامنة والمتبقية).
- خرائط حرارية.
- تم تصنيف المخاطر (مثل: الفشل التقني، التلاعب، الخطأ البشري، ضعف الرقابة).
- اعتماد معايير دولية مثل ISO، COSO ERM، PCI DSS.
- استخدام طرق حسابية (المتوسط، المنوال) لتحديد درجة الخطر النهائي، مع إعطاء أوزان للأراء المختلفة.

3. النتائج والتوصيات:

- بناء نموذج متكامل لتقييم المخاطر التشغيلية الخاصة ببطاقات الدفع.
- تحديد مواطن الضعف الحرجة واقتراح خطط تصحيحية ذكية. (SMART)
- دعم اتخاذ القرار من خلال التمثيل البصري والنمذجة.
- تأكيد أهمية المقاربة التشاركية في الوصول إلى تقييم دقيق وواقعي.

هذا الجانب يبرهن على إمكانية تطبيق الأطر النظرية والأدوات الرقمية الحديثة في بيئة مصرفية جزائرية، مع التأكيد على أهمية التحليل التشاركي والتكامل بين الملاحظة المباشرة والتحليل الكيفي في إدارة المخاطر التشغيلية.

4. مناقشة النتائج النهائية:

أظهرت الدراسة من خلال تطبيقها الميداني داخل بنك تراست الجزائر، أن اتباع مقاربة تشاركية ومنهجية دقيقة لتقييم المخاطر التشغيلية، يساهم بفعالية في تحسين فهم العمليات المرتبطة ببطاقات الدفع البنكية، ويُمكن المؤسسة من التعامل بمرونة أكبر مع التهديدات التشغيلية المحتملة إذ أن تحليل العمليات وتفكيكها إلى مهام فرعية، وتنظيم ورشات عمل تضم الفاعلين الميدانيين، أتاح للبنك رؤية أكثر واقعية للمخاطر ومواطن الضعف كما أن توظيف أنظمة رقمية متخصصة سمح بجمع وتحليل المعطيات بطريقة ديناميكية، ما مكن من رصد التكرار وشدة التأثير بدقة، وبالتالي دعم عملية اتخاذ القرار على أسس نوعية وقد تبين من خلال استخدام أدوات تقييم مثل مصفوفة المخاطر، أن هناك فرقاً واضحاً بين مستوى الخطر الخام والصافي، مما يعكس فعالية أنظمة الرقابة الحالية. هذا النهج المتكامل بين التحليل الكيفي والكمي، في إطار تنظيمي وتقني منسجم، أتاح إمكانية التخفيف من المخاطر بطريقة أكثر استباقية، وساهم في ترسيخ ثقافة مؤسساتية تُعلي من قيمة الرقابة والحوكمة التشغيلية، بما يعزز من أمن العمليات المالية وسلاستها دون الإخلال بمتطلبات الامتثال والفعالية.

خلاصة الجانب التطبيقي:

الجانب التطبيقي يُعد محوراً أساسياً في البحث، حيث تم الانتقال من التنظير إلى التطبيق العملي داخل بنك تراست الجزائر وقد ركز هذا الجانب على بطاقات الدفع البنكية باعتبارها من أكثر

المنتجات تعرضًا للمخاطر التشغيلية بسبب تعدد الجهات الفاعلة، وتشابك العمليات، والاعتماد المتزايد على الأنظمة الرقمية.

الخاتمة:

في ظل التحديات المتسارعة التي تشهدها البيئة المصرفية لا سيما في مجال أنظمة الدفع الإلكترونية تفرض المخاطر التشغيلية نفسها كأحد أهم محاور الانكشاف البنكي المعاصر وقد جاءت هذه الدراسة لتستجيب لهذه الضرورة عبر تحليل معمق لمخاطر بطاقات الدفع البنكية من خلال تجربة ميدانية داخل بنك ترست الجزائر مستندة إلى مقارنة بنائية ومنهج نوعي يزاوج بين الرؤية النظرية والتطبيق العملي.

تميز هذا العمل بتبني منهجية **RCSA** (التقييم الذاتي للمخاطر والرقابة) كأساس لتحديد وتصنيف وتقييم المخاطر التشغيلية وهي منهجية تفاعلية عززت من المشاركة الجماعية داخل البنك وسمحت برصد المخاطر من منظور داخلي واقعي. ولتعزيز فعالية هذه المنهجية،

تم توظيف تطبيق **RISK NUCLEUS** كأداة تقنية لدعم عملية النمذجة وتحليل النتائج، وتوليد خارطة مخاطر دقيقة وشاملة تعكس مستوى الخطورة والضوابط المقابلة لكل عملية مصرفية متعلقة ببطاقات الدفع.

وقد أظهرت نتائج البحث أن التحديات لا تكمن فقط في حجم وعدد المخاطر، بل في قدرتنا على قراءتها وفهم ديناميكيتها وتوقع تحولاتها وقد مكّن التكامل بين المنهجية والرقمنة من إحداث نقلة نوعية في التعامل مع المخاطر التشغيلية ليس باعتبارها تهديدات فقط بل كبؤر قابلة للإدارة والتحكم إذا ما تم تفعيل آليات الرقابة والتقييم الدوري بطريقة تشاركية ومدعومة تكنولوجياً.

إن هذه الدراسة بما حملته من تحليل واقعي وتوظيف لأدوات عملية لا تكفي بتقديم خارطة مخاطر موجهة لبنك ترست الجزائر فحسب، بل تقترح إطارًا مرجعيًا قابلاً للتكيف مع باقي المؤسسات المالية

الوطنية كما تفتح المجال أمام دراسات مستقبلية تبحث في دمج أدوات الذكاء الاصطناعي، والتعلم الآلي في منهجية RCSA بما يعزز التنبؤ بالمخاطر قبل وقوعها ويعزز الحوكمة الاستباقية. إن البحث في إدارة المخاطر التشغيلية هو رحلة مستمرة نحو بناء ثقافة مؤسسية قائمة على الوعي، التحليل، والاستجابة، وهذه الدراسة ليست إلا خطوة أولى في مسار طويل نحو مصرفية أكثر أمانًا وكفاءة واستدامة.

نتائج الجانب النظري

تناولت هذه الدراسة تحديدًا دقيقًا للمخاطر التشغيلية من خلال التمييز بينها وبين باقي أنواع المخاطر المصرفية، مع التركيز على أهميتها في بيئة رقمية متطورة. تم تحليل أبرز الأطر الدولية المعتمدة في إدارة هذه المخاطر مثل COSO ERM، ISO 31000، وبازل II وIII، مع التركيز على منهجية RCSA كنموذج تفاعلي تشاركي لتقييم المخاطر والضوابط الذاتية.

كما استعرض البحث الأدوات المعاصرة الداعمة مثل مؤشرات المخاطر الرئيسية (KRIs)، الخرائط الحرارية، وبطاقات التقييم، وتم تطبيق بعضها فعليًا باستخدام نظام RISK NUCLEUS داخل بنك ترست الجزائر لتصميم نموذج تقييم ديناميكي. ومن خلال مراجعة الأدبيات، تبيّن وجود فجوة في توظيف RCSA والأدوات الرقمية في البيئة المصرفية الجزائرية.

أكدت الدراسة أيضًا على أهمية البعد البياني في تقييم المخاطر، من خلال استخدام النمذجة والتمثيل البصري لدعم اتخاذ القرار، إلى جانب اعتماد مقاربة تشاركية شملت ورش عمل واستبيانات وملاحظة ميدانية لضمان شمولية التقييم ودقته.

نتائج الجانب التطبيقي

اعتمدت الدراسة على نمذجة مفصلة للعمليات التشغيلية المتعلقة ببطاقات الدفع، حيث تم تقسيمها إلى مراحل رئيسية تشمل: طلب البطاقة، تفعيلها، استخدامها، وتسوية العمليات، مع توثيق كل مرحلة وتحديد الجهات المعنية والمخاطر المحتملة.

تم تطبيق منهجية RCSA عبر تنظيم ورش عمل افتراضية ضمت موظفين من الأقسام المعنية، مدعومة باستبيانات شبه منظمة لتعزيز المشاركة وجمع بيانات دقيقة. وقد استند التحليل إلى مزيج من الخبرة الميدانية والمعطيات النوعية والتاريخية.

كما تم توظيف النسخة التجريبية من تطبيق RISK NUCLEUS لبناء خارطة مخاطر تفاعلية، شملت إنتاج مصفوفات تقييم تميز بين المخاطر الكامنة والمتبقية، وتوليد تقارير وخرائط حرارية توضح مكانم الخطر بدقة.

جرى تصنيف وتقييم المخاطر الأساسية المرتبطة بكل عملية، مثل الفشل التقني، الخطأ البشري، التلاعب، أو ضعف الرقابة، وفقاً لمعايير دولية مثل ISO و COSO و PCI DSS، مع اعتماد مصفوفات لقياس الأثر والاحتمالية.

تم اقتراح خطط تصحيحية ذكية (SMART) لمعالجة النقاط الحرجة، مع التركيز على تعزيز الضوابط في المراحل الحساسة من دورة حياة البطاقة.

أخيراً، سعت الدراسة إلى ترسيخ ثقافة المخاطر داخل البنك، من خلال إشراك الموظفين في التقييم ونشر نتائج الورشات داخلياً، بما يعزز الوعي المؤسسي ويساهم في التحسين المستمر لإدارة المخاطر التشغيلية.

الاقتراحات الخاصة بالدراسة:

توصي الدراسة بتريسيخ منهجية RCSA داخل البنك من خلال تطبيقها بشكل دوري ومنهجي على مختلف العمليات المرتبطة ببطاقات الدفع، مع إشراك كافة الأطراف المعنية مثل المديرين، الموظفين، ووحدة الرقابة الداخلية، لضمان تقييم واقعي وفعال للمخاطر والضوابط.

كما يُقترح تحسين استخدام تطبيق RISK NUCLEUS عبر توسيع مجالاته لتشمل إدارة خطط العمل، مراقبة مؤشرات المخاطر الرئيسية (KRIs)، وتوليد تقارير تحليلية تدعم اتخاذ القرار الاستراتيجي. في الجانب التقني، تبرز الحاجة إلى تعزيز جاهزية الأنظمة من خلال تطوير بنية احتياطية تضمن استمرارية الخدمة، وتحسين بروتوكولات الاتصال لضمان سرعة وكفاءة المعالجة، خاصة في حالات الأعطال.

أما من حيث الأمن السيبراني، فتوصي الدراسة بتفعيل استراتيجيات متقدمة تشمل دمج تقنيات الذكاء الاصطناعي في كشف الاحتيال، وتطبيق أنظمة المصادقة المتعددة مثل FA2، مع رفع الوعي الأمني لدى الموظفين والعملاء.

وفيما يخص الامتثال التنظيمي، يجب مراجعة السياسات الداخلية المتعلقة بأمان الدفع بما ينسجم مع المعايير الدولية مثل PCI-DSS، ISO 27001، ومعايير مكافحة غسل الأموال.

ومن المقترحات المهمة كذلك ربط تقييم المخاطر الناتج عن RCSA بأداء البنك التشغيلي، واعتماده في صياغة الأهداف وتخطيط الأعمال، مما يساهم في تكامل إدارة المخاطر مع الرؤية الاستراتيجية للمؤسسة.

وتعزيزاً لهذا التوجه، توصي الدراسة بإطلاق برامج تدريبية دورية تشمل المحاكاة العملية والتدريب على أدوات التحليل الحديثة، إلى جانب تطوير نظام إنذار مبكر داخلي يستند إلى مؤشرات تحذيرية مشتقة من نتائج الورشات والتقارير التفاعلية داخل RISK NUCLEUS.

آفاق الدراسة:

تُفتح هذه الدراسة آفاقاً مستقبلية هامة على المستويين الأكاديمي والتطبيقي لما لها من قابلية للتوسيع والتطوير ضمن سياق إدارة المخاطر التشغيلية في البيئة المصرفية الجزائرية فمن جهة أولى يمكن توسيع نطاق البحث ليشمل خدمات رقمية أخرى مثل القروض الإلكترونية، الحسابات الجارية الرقمية والمعاملات عبر التطبيقات المصرفية مما يسمح بإعداد خارطة مخاطر تشغيلية شاملة تغطي مختلف أبعاد النشاط البنكي الرقمي.

ومن جهة ثانية تبرز إمكانية تطوير نموذج تقييمي موحد على المستوى الوطني يركز على منهجية RCSA ويستفيد من أدوات التحليل الرقمي كـ RISK NUCLEUS، بما يتيح تعميم التجربة على مؤسسات مالية أخرى. كما يُمكن استثمار تقنيات الذكاء الاصطناعي، لا سيما التعلم الآلي، لتعزيز قدرة البنوك على التنبؤ بالمخاطر قبل وقوعها والتعامل معها بفعالية أكبر.

وتتترح الدراسة في هذا الإطار العمل على بناء منصة رقمية تفاعلية خاصة بتسيير ورشات تقييم المخاطر، تسمح بتنفيذ تقييمات جماعية بشكل رقمي، تربط بين الأداء التشغيلي، مؤشرات المخاطر، ونقاط الضعف في الضوابط. بالإضافة إلى ذلك، يُمكن إنجاز دراسات مقارنة مستقبلية مع بنوك في بلدان ذات بيئات اقتصادية وتنظيمية مشابهة (مثل تونس، مصر)، مما يعزز تبادل الخبرات ويُسهّم في قياس نضج ممارسات إدارة المخاطر.

وفي الأخير، تُعد هذه الدراسة مساهمة أولية يمكن الاستفادة منها في دعم صناع القرار والهيئات التنظيمية على المستوى الوطني، لتطوير سياسات مصرفية مبنية على تحليل المخاطر، تواكب التحولات الرقمية المتسارعة وتستجيب للتحديات التقنية والأمنية الراهنة.

المراجع و المصادر

قائمة المراجع

الكتب:

- Bellini, A. (2016).** *Operational Risk Management: A Practical Approach to Intelligent Data Analysis*. Springer.
- Bessis, J. (2015).** *Risk Management in Banking (4th ed.)*. Wiley.
- Collier, P. (2009).** *Fundamentals of Risk Management for Accountants and Managers*. Elsevier.
- Cruz, M. (2002).** *Modeling, Measuring and Hedging Operational Risk*. Wiley.
- Girling, P. (2013).** *Operational Risk Management: A Complete Guide for Banking and FinTech*. Wiley.
- Gregoriou, G. (2009).** *Operational Risk Toward Basel III: Best Practices and Issues in Modeling, Management, and Regulation*. Wiley.
- Laycock, M. (2014).** *Risk Management at the Top: A Guide to Risk and Its Governance in Financial Institutions*. Wiley.
- Loader, D. (2006).** *Operational Risk: Regulation, Analysis and Management*. Butterworth-Heinemann.
- Onyiriuba, L. (2016).** *Bank Risk Management in Developing Economies*. Academic Press.

المقالات والأوراق البحثية:

- Agarwal, R., & Dhar, V. (2014).** *Big Data, AI, and Operational Risk in Financial Services*. *Journal of Financial Regulation and Compliance*, 22(3), 187–202.
- Arora, P., & Rahman, A. (2018).** *Regulatory Compliance and Risk Management in Digital Payments*. *International Journal of Banking & Finance*, 12(2), 54–78.
- Chernobai, A., Jorion, P., & Yu, F. (2010).** *The Determinants of Operational Risk in Banks: A Cross-country Analysis*. *Journal of Banking & Finance*, 34(5), 823–837.
- Kumar, S., & Singh, R. (2020).** *Fraud Detection in Payment Systems Using Machine Learning Techniques*. *Journal of Banking Technology*, 15(1), 50–65.
- Mebarki, R., & Benali, R. (2022).** *Risk Assessment Methods in Algerian Banks*. *Algerian Journal of Economic Studies*, 8(1), 45–62.

Mishra, P., & Gupta, V. (2022). *Cybersecurity Challenges and Solutions for Banking Payments.* Journal of Financial Innovation, 10(2), 112–130.

Nguyen, T., & Tran, L. (2019). *The Role of Regulatory Frameworks in Reducing Operational Risk in Digital Payments.* Banking & Finance Review, 17(4), 89–105.

Zarif, T., & Hossain, M. (2020). *Risk Categorization in Financial Institutions.* Finance Research Letters, 15(3), 77–85.

Zhang, Y., & Wang, J. (2019). *Internal Audit and Organizational Compliance in Financial Institutions.* Journal of Financial Ethics, 11(2), 33–50

التقارير والمعايير والأطر المرجعية:

Banque d’Algérie. (2011). *Regulations on Internal Control and Risk Management in Algerian Banks.* Algerian Banking Authority.

Banque d’Algérie. (2014). *Financial Stability Report.* Algerian Banking Authority.

Basel Committee on Banking Supervision (BCBS). (2003–2019). *Various Reports and Principles on Operational Risk.* Bank for International Settlements.

CGAP. (2008). *Human Resources and Operational Risk.*

COSO. (2013, 2017). *Internal Control – Integrated Framework & ERM Framework.* Committee of Sponsoring Organizations of the Treadway Commission.

Deloitte. (2020, 2023). *Risk Management and Financial Transparency in Banking Sector.* Deloitte Insights.

IOR (Institute of Risk Management). (2021). *Guide to Risk Scorecards.*

ISO. (2018, 2019, 2021). *31000, 22301, 37301 Standards on Risk and Compliance Management.* International Organization for Standardization.

KPMG. (2019). *Trends in Banking Risk Management and Compliance.* KPMG International.

MicroSave. (2011). *Disaster and Operational Risk in Microfinance.*

Secureframe. (n.d.). *Modern Compliance Frameworks for Financial Institutions.*

SPTF. (2016). *Responsible Financial Performance Standards.*

Trust Bank Algeria. (2023). *Operational Incident Data (بيانات داخلية).*

الملاحق

الملحق 1: العائلات السبع للمخاطر حسب لجنة بازل.

Catégorie de risque	Sous catégorie de risque
Fraude interne Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'enfreintes à la législation ou aux règles de l'entreprise qui implique au moins une personne en interne	Activité non autorisée
	Vol et fraude (interne)
Fraude externe Pertes dues à un acte intentionnel de fraude, de détournement de biens, d'enfreintes à la législation par une tierce partie	Vol et fraude (externe)
	Sécurité des systèmes (fraude externe)
	Sécurité du lieu de travail

<p><i>Pratiques en matière d'emploi et sécurité sur le lieu de travail</i></p> <p>Pertes résultant d'actes incompatibles au regard de la loi en matière d'emploi, de législation relative à la santé ou à la sécurité, du paiement d'indemnités ou de discrimination sociale</p>	<p>Relations de travail</p> <p>Egalité et discrimination</p> <p>Gestion des ressources humaines</p>
<p>Clients, produits et pratiques commerciales</p> <p>Pertes résultant d'un acte non intentionnel ou d'une négligence dans l'exercice d'une obligation professionnelle face au client (incluant les exigences en matière fiduciaire et de suitability*) ou pertes résultant dans la nature ou la conception d'un produit</p>	<p>Conformité, diffusion d'informations et devoir fiduciaire</p> <p>Services conseils</p>
<p><i>Dommmages aux actifs corporels</i></p>	

Pertes résultant de la perte ou du dommage sur un actif corporel à la suite d'une catastrophe naturelle ou d'un autre sinistre

Catastrophes
et autres
sinistres

Dysfonctionnements de l'activité et des systèmes

Pertes résultant d'une interruption des activités ou une panne système

Systemes

Exécution, livraison et gestion des processus

Pertes résultant d'une anomalie de traitement ou des relations avec la contrepartie entrant en jeu ou avec le vendeur

Saisie,
exécution et
suivi des
transactions

Surveillance
et notification
financière

	Admission et documentation clientèle
	Gestion des comptes clients
	Contreparties commerciales
	Fournisseurs