

جامعة ميدأوشن



كلية الإدارة

قسم / تخصص. ماجستير إدارة المخاطر

عنوان البحث

أثر التحول الرقمي على إدارة المخاطر التشغيلية في البنوك : دراسة ميدانية

على العمليات المصرفية في البنوك السعودية

إعداد الطالب / أيمن حسين بارعيده

إشراف/

د. الفیصل عبد الحمید محمد

دفايز علي الجراد

العام الدراسي:

٢٠٢٥

	جدول المحتويات
١	الفصل الأول
٥	ملخص الدراسة
٧	مقدمة الدراسة
٨	مشكلة الدراسة
٩	أهمية الدراسة
١٠	أهداف الدراسة
١٢	تساؤلات الدراسة
١٣	فرضيات الدراسة
١٤	مصطلحات الدراسة
١٥	متغيرات الدراسة
١٦	الفصل الثاني
١٧	الدراسات السابقة
٢٣	الإطار النظري
٢٥	الإطار المفاهيمي للمخاطر التشغيلية

٣٠	الإطار التنظيمي لإدارة المخاطر (لجنة بازل)
٣٤	مفاهيم ونماذج التحول الرقمي (Digital Transformation)
٣٨	تطبيقات التحول الرقمي في العمليات المصرفية
٤٠	الأثر المزدوج للتحول الرقمي على المخاطر التشغيلية
٤٤	إدارة المخاطر السيبرانية ومخاطر تقنية المعلومات
٤٨	مخاطر الطرف الثالث (Third-Party Risk) والشركات التقنية المالية (FinTech)
٤٩	توظيف التقنيات الرقمية في تعزيز فاعلية ORM
٥٠	البيئة التنظيمية والرقابية في المملكة العربية السعودية
٥٣	الخاتمة
٥٤	الفصل الثالث
٥٥	منهجية الدراسة
٥٥	مجتمع الدراسة
٥٦	أدوات جمع البيانات
٥٧	حدود الدراسة

٥٨	الاستبيان
٦٦	الفصل الرابع
٦٧	التحليل الإحصائي
٧٣	النتائج
٧٥	التوصيات
٧٩	المراجع
٨٥	الملخص
٨٦	الملاحق

ملخص الدراسة (Abstract)

هدفت هذه الدراسة إلى تقييم الأثر الصافي للتحويل الرقمي على فاعلية وكفاءة إدارة المخاطر التشغيلية في العمليات المصرفية بالبنوك السعودية. اعتمدت الدراسة على المنهج الوصفي التحليلي، وتمثلت أداة جمع البيانات في استبيان وُزع على عينة قسدية من (100) مختص في إدارات المخاطر والعمليات وتقنية المعلومات بالبنوك السعودية. أظهرت النتائج الإحصائية الرئيسية ما يلي:

1. قبول الفرضية الرئيسية: أثبتت الدراسة وجود أثر إيجابي وقوي ذي دلالة إحصائية للتحويل الرقمي على فاعلية إدارة المخاطر التشغيلية (معامل ارتباط $R=0.758$)، حيث يساهم التحويل الرقمي في تحسين كفاءة آليات الرقابة والكشف عن المخاطر.
2. التحدي الأبرز: أكد المشاركون أن ظهور وتفاقم المخاطر السيبرانية هو الأثر السلبي الأبرز المصاحب للرقمنة، مما يفرض ضغوطاً متزايدة على أطر إدارة المخاطر.
3. مكسب الكفاءة: يوجد إجماع على أن التحويل الرقمي ينجح في تقليل الأخطاء التشغيلية اليدوية الناتجة عن العنصر البشري بشكل كبير، مما يعزز الاستقرار التشغيلي.

4. دور التقنيات: ساهمت أنظمة المراقبة الآلية المعتمدة على الذكاء الاصطناعي في

تحسين الكشف المبكر عن المخاطر وتقليص زمن الاستجابة للحوادث.

بناءً على النتائج، أوصت الدراسة البنوك بضرورة تبني مبدأ "المخاطر في التصميم"

(Risk by Design) في تطوير المنتجات الرقمية، ورفع مستوى الاستثمار في الأمن

السيبراني، وتطوير برامج تدريب متخصصة تجمع بين الجوانب التكنولوجية والرقابية

لمواجهة التحديات الجديدة في العصر الرقمي.

مقدمة الدراسة

شهد القطاع المصرفي العالمي والمحلي تحولات جذرية في العقدين الأخيرين، مدفوعة بالتقدم التكنولوجي المتسارع وثورة التحول الرقمي. لم يعد العمل المصرفي مقتصرًا على الفروع التقليدية، بل أصبح يعتمد بشكل متزايد على المنصات الرقمية، تطبيقات الهاتف المحمول، الذكاء الاصطناعي، وتحليلات البيانات الضخمة (Big Data). هذا التحول، الذي يهدف إلى تعزيز الكفاءة التشغيلية وتحسين تجربة العميل، يفرض تحديات جديدة ومعقدة على إدارة المخاطر.

تُعدّ المخاطر التشغيلية - الناتجة عن فشل العمليات الداخلية أو الأفراد أو الأنظمة أو الأحداث الخارجية - من أبرز مصادر الخسارة المحتملة للبنوك، خاصة في البيئة الرقمية المتزايدة التعقيد. فبينما يفتح التحول الرقمي آفاقاً واسعة للابتكار، فإنه في الوقت ذاته يخلق أنواعاً مستحدثة من المخاطر، مثل مخاطر الأمن السيبراني، ومخاطر تعطل الأنظمة، ومخاطر الذكاء الاصطناعي غير المنضبط، ومخاطر حوكمة البيانات.

تأتي هذه الدراسة لتسليط الضوء على هذه العلاقة المتبادلة والمتشابكة بين شقي المعادلة: التحول الرقمي وإدارة المخاطر التشغيلية. وتهدف إلى تحليل وتقييم الكيفية التي أثر بها تبني البنوك السعودية للتقنيات الرقمية المتقدمة على طبيعة وحجم وكيفية إدارة المخاطر

التشغيلية في عملياتها المصرفية، سعياً لتقديم إطار عمل مستدير يدعم صناع القرار في الحفاظ على استقرار وسلامة القطاع المصرفي في المملكة.

مشكلة الدراسة

تتبع مشكلة الدراسة من التناقض الظاهري بين هدف التحول الرقمي المعلن (وهو تحسين الكفاءة وتقليل الأخطاء البشرية) وبين ما يرافقه في الواقع من ظهور أنواع جديدة ومتطورة من المخاطر التشغيلية التي قد تفوق في خطورتها المخاطر التقليدية. وعلى الرغم من الجهود المبذولة، لا يزال هناك قصور في الفهم الشامل والتقييم الدقيق للأثر الصافي للتحول الرقمي على منظومة إدارة المخاطر التشغيلية في البنوك العاملة في بيئة اقتصادية متغيرة ومحفزة للرقمنة مثل المملكة العربية السعودية.

المشكلة الرئيسية:

ما هو الأثر الصافي (الإيجابي والسلبي) للتحول الرقمي على فعالية وكفاءة إدارة المخاطر التشغيلية في العمليات المصرفية بالبنوك السعودية؟

الأسئلة الفرعية المنبثقة:

1. ما مدى تبني وتطبيق أدوات وتقنيات التحول الرقمي (مثل الذكاء الاصطناعي، الحوسبة السحابية، والبيانات الضخمة) في العمليات المصرفية بالبنوك السعودية؟

2. كيف أثر التحول الرقمي على طبيعة ونوعية المخاطر التشغيلية التي تواجه البنوك

(مثل مخاطر الأمن السيبراني، مخاطر الطرف الثالث، ومخاطر استمرارية

الأعمال)؟

3. ما هو دور أدوات التحول الرقمي في تعزيز كفاءة وفعالية آليات إدارة المخاطر

التشغيلية (مثل نماذج قياس الخسائر، ومؤشرات المخاطر الرئيسية KRI's،

وعمليات الرقابة الداخلية)؟

4. ما هي التحديات الرئيسية التي تواجه البنوك السعودية في تكيف أطرها الحالية

لإدارة المخاطر التشغيلية لتتوافق مع بيئة العمل الرقمية الجديدة؟

أهمية الدراسة

الأهمية العلمية (الأكاديمية)

1. سد الفجوة المعرفية: تساهم الدراسة في إثراء المكتبة العربية ببحث تطبيقي يربط

بشكل مباشر بين متغيرين حيويين هما التحول الرقمي وإدارة المخاطر التشغيلية،

وهو ما يمثل نقصاً في الدراسات الميدانية المحلية التي تركز على القطاع

المصرفي السعودي.

2. تطوير الإطار النظري: تساعد نتائج الدراسة في تطوير الإطار النظري لمفاهيم

إدارة المخاطر التشغيلية الحديثة (Operational Risk Management -)

(ORM) من خلال تقديم أدلة تجريبية حول كيفية إعادة تشكيل المخاطر وتصنيفها في العصر الرقمي.

3. توفير مرجع للباحثين: توفر الدراسة بيانات ومعلومات تحليلية دقيقة يمكن أن

تكون بمثابة نقطة انطلاق وأساس للباحثين والأكاديميين المهتمين بدراسة

التكنولوجيا المالية (FinTech)، والحوكمة، والامتثال في البيئة المصرفية.

الأهمية العملية (التطبيقية)

1. دعم صنّاع القرار والمشرعين: تُقدم نتائج الدراسة توصيات عملية ومبنية على

الأدلة للمؤسسات الرقابية (مثل البنك المركزي السعودي) وإدارات المخاطر العليا

في البنوك، لمساعدتهم في تطوير سياسات وإجراءات أكثر فاعلية لإدارة المخاطر

الرقمية المستجدة.

2. تحسين الكفاءة التشغيلية: تساعد الدراسة البنوك على تحديد نقاط الضعف في

عملياتها الرقمية التي تزيد من احتمالية حدوث خسائر تشغيلية، مما يمكنها من

توجيه استثماراتها نحو تعزيز الضوابط الرقابية وتطوير أنظمة الحماية السيبرانية.

3. تعزيز التنافسية والاستقرار: من خلال فهم الأثر الحقيقي للتحول الرقمي على

المخاطر، يمكن للبنوك السعودية اتخاذ قرارات استراتيجية مدروسة، مما يعزز

قدرتها التنافسية ويساهم في استقرار النظام المالي في المملكة تماشياً مع رؤية

2030.

أهداف الدراسة

تهدف الدراسة بشكل عام إلى تقييم وتحليل الأثر الكلي (الإيجابي والسلبي) لتبني التحول الرقمي على منظومة إدارة المخاطر التشغيلية في البنوك السعودية، ويمكن تفصيل هذه الأهداف على النحو التالي:

الهدف الرئيسي

تقييم وتحليل الأثر الصافي للتحول الرقمي على فاعلية وكفاءة إدارة المخاطر التشغيلية في العمليات المصرفية بالبنوك السعودية.

الأهداف الفرعية

1. تحديد مستوى تبني وتطبيق البنوك السعودية لأدوات وتقنيات التحول الرقمي الحديثة (كالذكاء الاصطناعي والبيانات الضخمة) في تنفيذ عملياتها المصرفية.
2. الكشف عن التغيرات التي طرأت على طبيعة ونوعية المخاطر التشغيلية (مثل المخاطر السيبرانية ومخاطر استمرارية الأعمال) نتيجة للتحول الرقمي.
3. قياس دور أدوات التحول الرقمي في دعم وتحسين كفاءة آليات إدارة المخاطر التشغيلية (كأنظمة المراقبة الآلية ونماذج قياس المخاطر).
4. تحديد أبرز التحديات التي تواجه إدارات المخاطر في البنوك السعودية عند محاولة مواءمة أطرها الحالية مع متطلبات البيئة التشغيلية الرقمية الجديدة.

تساؤلات الدراسة (الأسئلة البحثية)

التساؤل الرئيسي

ما هو الأثر الصافي للتحويل الرقمي على فاعلية وكفاءة إدارة المخاطر التشغيلية في العمليات المصرفية بالبنوك السعودية؟

التساؤلات الفرعية

1. ما هو مستوى تطبيق أدوات وتقنيات التحويل الرقمي في العمليات المصرفية

بالبنوك السعودية؟

2. ما التغيرات التي أحدثها التحويل الرقمي على طبيعة ونوعية المخاطر التشغيلية

التي تواجه البنوك؟

3. إلى أي مدى تساهم أدوات التحويل الرقمي في تعزيز كفاءة آليات إدارة المخاطر

التشغيلية؟

4. ما هي أبرز التحديات التي تواجه البنوك السعودية في تكييف أطر إدارة المخاطر

التشغيلية مع البيئة الرقمية؟

3. فرضيات الدراسة

الفرضية الرئيسية H_1

يوجد أثر ذو دلالة إحصائية للتحول الرقمي على فاعلية وكفاءة إدارة المخاطر التشغيلية في العمليات المصرفية بالبنوك السعودية.

الفرضيات الفرعية

1. يوجد أثر ذو دلالة إحصائية لتبني أدوات التحول الرقمي على انخفاض المخاطر التشغيلية التقليدية.

2. يوجد أثر ذو دلالة إحصائية لتبني أدوات التحول الرقمي على ظهور وزيادة حدة المخاطر التشغيلية المستحدثة (مثل الأمن السيبراني).

3. تساهم أدوات التحول الرقمي (مثل الذكاء الاصطناعي) في رفع كفاءة آليات تحديد وقياس ومراقبة المخاطر التشغيلية في البنوك.

4. يوجد علاقة عكسية بين مستوى مواعمة أطر إدارة المخاطر التشغيلية مع البيئة الرقمية وحجم الخسائر التشغيلية الناتجة عن فشل الأنظمة.

مصطلحات الدراسة

المصطلح	التعريف الإجرائي في سياق الدراسة
التحول الرقمي (Digital Transformation)	يُقصد به في هذا البحث، عملية دمج التقنيات الرقمية المتقدمة (مثل الحوسبة السحابية، الذكاء الاصطناعي، والتعلم الآلي) في كافة جوانب العمليات المصرفية، بهدف تغيير كيفية تقديم الخدمات وزيادة الكفاءة التشغيلية.
إدارة المخاطر التشغيلية (Operational Risk) (Management – ORM)	هي مجموعة الإجراءات والعمليات التي تستخدمها البنوك لتحديد، قياس، مراقبة، والتحكم في المخاطر الناتجة عن فشل العمليات الداخلية أو الأفراد أو الأنظمة أو الأحداث الخارجية، وتُقاس بفاعلية الضوابط الداخلية ونسبة انخفاض الخسائر التشغيلية غير المتوقعة.
العمليات المصرفية (Banking Operations)	هي الأنشطة الأساسية التي تقوم بها البنوك، وتشمل على سبيل المثال لا الحصر: تقديم القروض، إدارة الحسابات والودائع، عمليات الدفع والتحويلات، وخدمات التمويل التجاري، وتحديدًا تلك العمليات التي تم تحويلها إلى قنوات رقمية.

البنوك السعودية (Saudi Banks)	هي البنوك التجارية التي تعمل ضمن نطاق المملكة العربية السعودية وتخضع لإشراف ورقابة البنك المركزي السعودي (SAMA).
--------------------------------	--

متغيرات الدراسة

تعتمد الدراسة على متغيرين رئيسيين لقياس العلاقة بينهما:

نوع المتغير	المتغير	المؤشرات الرئيسية (الأبعاد)
المتغير المستقل	التحول الرقمي (Digital Transformation)	1. مستوى تبني تقنيات الذكاء الاصطناعي والتعلم الآلي. 2. مدى استخدام الحوسبة السحابية (Cloud Computing). 3. تطبيق حلول البيانات الضخمة (Big Data) والتحليلات المتقدمة.
المتغير التابع	فاعلية إدارة المخاطر التشغيلية (ORM Effectiveness)	1. كفاءة الضوابط الداخلية ونظم الرقابة.

2. درجة الاستجابة للمخاطر المستحدثة (مثل مخاطر الأمن السيبراني). 3. دقة نماذج قياس وتوقعات الخسائر التشغيلية. 4. مدى امتثال البنك للمعايير الدولية (مثل بازل III).		
---	--	--

الفصل الثاني

الدراسات السابقة

1. دراسة زهر ومحمد وحامد (2024)

العنوان: "أثر التحول الرقمي على إدارة المخاطر المصرفية دراسة حالة"

- **الهدف:** تحليل انعكاسات مؤشرات التحول الرقمي على إدارة المخاطر المصرفية في البنك التجاري الدولي خلال الفترة 2017-2021.
- **المنهج والأداة:** التحليل الإحصائي.
- **أهم النتائج:** توصلت الدراسة إلى أن هناك فروق ذات دلالة إحصائية للتحول الرقمي على إدارة مخاطر السوق، وإدارة مخاطر الائتمان، وإدارة مخاطر التشغيل.

2. دراسة الخفاجي (2017)

العنوان: "تفعيل إدارة المخاطر المصرفية في ظل تكنولوجيا المعلومات والاتصالات"

- **الهدف:** إبراز أهمية تفعيل إدارة المخاطر المصرفية في عصر تكنولوجيا المعلومات والاتصالات لتطوير الأداء والمحافظة على القدرة التنافسية.
- **أهم النتائج والتوصيات:** بينت الدراسة أهداف إدارة المخاطر المصرفية والمخاطر الناتجة عن التطور التكنولوجي. وأوصت بضرورة الاعتماد على الوسائل الحديثة والتطورات التكنولوجية لتقليل الأخطار، ومراقبة التغيرات في البيئة الخارجية، والاهتمام بالتدريب المستمر.

3. دراسة العبد الله (2021)

العنوان: "دور حوكمة تكنولوجيا المعلومات في الحد من المخاطر المصرفية الإلكترونية:

دراسة ميدانية"

• **الهدف:** توضيح دور حوكمة تكنولوجيا المعلومات في الحد من مخاطر العمليات

المصرفية الإلكترونية في البنوك التجارية بما يضمن تحسين أداء البنوك.

• **أهم النتائج:** توصلت الدراسة إلى أن تطبيق حوكمة تكنولوجيا المعلومات يؤدي

إلى الحد من المخاطر المصرفية الإلكترونية، وأن نظام الرقابة الداخلية يدعم هذه

الحوكمة في ظل إطار COBIT.

4. دراسة شكر (2024)

العنوان: "دور تقنيات الذكاء الاصطناعي في تعزيز تطبيق إطار (COSO) الرقابة

الداخلية لإدارة المخاطر التشغيلية في صناعة البنوك وأثره على الأداء المالي"

• **الهدف:** استكشاف استخدامات الذكاء الاصطناعي كأحد الأساليب الحديثة التي

تعزز الأداء المالي، وتوضيح دور الرقابة الداخلية في إدارة المخاطر التشغيلية.

• **المنهج والأداة:** المنهج الوصفي التحليلي، باستخدام استبيان وُزِعَ على عينة

عشوائية من موظفي البنوك.

• **أهم النتائج:** وجود تأثير ذي دلالة معنوية للذكاء الاصطناعي في تعزيز إطار

COSO للرقابة الداخلية في إدارة المخاطر التشغيلية، مما يساهم في تحسين أداء

قطاع المصارف.

5. دراسة النعساني (2024)

العنوان: "أثر استخدام تطبيقات الذكاء الاصطناعي في تخفيف المخاطر في العمليات

المصرفية"

• **الهدف:** إبراز أثر استخدام تطبيقات الذكاء الاصطناعي في الحد من مخاطر

الأعمال المصرفية، وإعادة هندسة الأعمال، وحماية المصارف من التعثر، ومعرفة

واقع تطبيق هذه التقنيات ومعوقاتها.

• **المنهج والأداة:** المنهج الوصفي التحليلي، تم التطبيق على عينة من المصارف

العاملة في المملكة العربية السعودية.

• **أهم النتائج:** لتطبيقات الذكاء الاصطناعي دور مهم في الحد من مخاطر الأعمال

المصرفية، إلا أن الاستخدام الفعلي لا يزال محدوداً بسبب وجود معوقات فنية

ومعلوماتية ونقص في المتخصصين.

6. دراسة الحجرف (2024)

العنوان: "دور الذكاء الاصطناعي في تعزيز الأمن السيبراني رؤى نظرية"

• **الهدف:** التعرف على أبرز مجالات وتطبيقات الذكاء الاصطناعي المستخدمة في تحسين الأمن السيبراني وبيان التحديات.

• **المنهج والأداة:** المنهج الوصفي، الدراسة النظرية.

• **أهم النتائج:** تقنيات الذكاء الاصطناعي تساهم في تحسين كفاءة استراتيجيات

الأمن السيبراني عبر التنبؤ بالتهديدات والاستجابة السريعة. وأوصت بضرورة

تدريب الموارد البشرية وتطوير إطار قانوني وأخلاقي لاستخدام التكنولوجيا بشكل

مسؤول.

7. دراسة بن علي (2023)

العنوان: "مساهمة الذكاء الاصطناعي في الكشف عن الاحتيال في القطاع المصرفي

باستخدام تطبيق الأمن السيبراني بنك Danske الدنماركي أنموذجاً"

• **الهدف:** إبراز مساهمة الذكاء الاصطناعي في الكشف عن الاحتيال في القطاع

المصرفي باستخدام تطبيق الأمن السيبراني.

• **المنهج والأداة:** المنهج الوصفي التحليلي، دراسة حالة لتجربة بنك Danske

الدنماركي.

• **أهم النتائج:** ساهم تطبيق كشف الاحتيال والأمن السيبراني المعتمد على الذكاء

الاصطناعي في بنك Danske في الكشف عما نسبته 50% من الاحتيال

الفعلي.

العنوان: "دور الذكاء الاصطناعي في تحسين أداء الخدمات المصرفية"

- **الهدف:** التعرف على دور الذكاء الاصطناعي في أداء الخدمات المصرفية.
- **المنهج والأداة:** المنهج الوصفي التحليلي، الدراسة النظرية.
- **أهم النتائج والتوصيات:** ساهم تطبيق الذكاء الاصطناعي في تطوير أداء المصارف، تحسين جودة الخدمة، التحكم في التكاليف، تخفيف المخاطر، وزيادة الإيرادات. وأوصت الدراسة بأهمية تطبيق المزيد من برامج وتطبيقات الذكاء الاصطناعي.

الإطار النظري

المحور الأول: الإطار المفاهيمي للمخاطر التشغيلية (Operational Risk)

- تعريف المخاطر التشغيلية وفقاً لـ "بازل" والمفاهيم الأكاديمية.
- تصنيفات المخاطر التشغيلية (فشل الأفراد، فشل العمليات، فشل الأنظمة، الأحداث الخارجية).
- مكونات عملية إدارة المخاطر التشغيلية (التحديد، القياس، المراقبة، التخفيف).
- مفهوم الخسائر التشغيلية وأنواعها (مباشرة وغير مباشرة).

المحور الثاني: الإطار التنظيمي لإدارة المخاطر (لجنة بازل)

- اتفاقيات بازل (II و III) ودورها في تعزيز إدارة المخاطر التشغيلية عالمياً.
- الطرق المعتمدة لقياس رأس المال مقابل المخاطر التشغيلية (الطريقة الأساسية، طريقة المؤشرات القياسية، طريقة القياس المتقدمة).
- متطلبات الحوكمة والضوابط الداخلية في ضوء إرشادات بازل.

المحور الثالث: مفاهيم ونماذج التحول الرقمي (Digital Transformation)

- التعريف الشامل للتحول الرقمي وخصائصه في القطاع المالي.

- مقارنة بين الرقمنة (Digitization)، والأتمتة (Automation)، والتحول الرقمي.
- الركائز التكنولوجية للتحول الرقمي (الذكاء الاصطناعي، الحوسبة السحابية، البيانات الضخمة).
- نماذج تبني التحول الرقمي في المؤسسات المالية.

المحور الرابع: تطبيقات التحول الرقمي في العمليات المصرفية

- استخدام الذكاء الاصطناعي (AI) في أتمتة العمليات الأساسية (التعرف على العملاء، معالجة القروض).
- دور البيانات الضخمة (Big Data Analytics) في اتخاذ القرارات المصرفية وتحسين تجربة العميل.
- تأثير تقنية البلوك تشين (Blockchain) على الشفافية وكفاءة التسوية المصرفية.
- تحول قنوات الخدمة (من الفرع التقليدي إلى المنصات الرقمية).

المحور الخامس: الأثر المزدوج للتحول الرقمي على المخاطر التشغيلية

- الأثر الإيجابي: دور الرقمنة في تقليل الأخطاء البشرية، وتحسين دقة المعالجة، وزيادة سرعة العمليات.
- الأثر السلبي (المخاطر المستحدثة): ظهور مخاطر جديدة غير تقليدية ناتجة عن تعقيد الأنظمة التكنولوجية.

- التحليل المقارن بين المخاطر التشغيلية التقليدية والمخاطر التشغيلية في البيئة الرقمية.

المحور السادس: إدارة المخاطر السيبرانية ومخاطر تقنية المعلومات

- تعريف المخاطر السيبرانية (Cyber Risk) ومصادرها في البنوك.
 - مخاطر استمرارية الأعمال (Business Continuity Risk) والتعافي من الكوارث في الأنظمة الرقمية.
 - مخاطر البنية التحتية التكنولوجية وفشل الأنظمة.
 - استراتيجيات التخفيف من المخاطر السيبرانية في البيئة المصرفية.
- المحور السابع: مخاطر الطرف الثالث (Third-Party Risk) والشركات التقنية المالية (FinTech)

- مفهوم مخاطر الطرف الثالث وأهميته في ظل الاعتماد المتزايد على الحوسبة السحابية وشركات الـ FinTech.
- إدارة مخاطر سلسلة التوريد التكنولوجية والمقاولين الخارجيين.
- آليات تقييم ومراقبة الالتزام التنظيمي للشركات التكنولوجية المتعامل معها.

المحور الثامن: توظيف التقنيات الرقمية في تعزيز فاعلية ORM

- دور الذكاء الاصطناعي في المراقبة الآلية واكتشاف الاحتيال والشذوذ (Fraud Detection).
- استخدام التعلم الآلي في بناء نماذج قياس وتوقع الخسائر التشغيلية بدقة أعلى.
- الاستفادة من تحليلات البيانات الضخمة لتحديد مؤشرات المخاطر الرئيسية (KRIs) في الوقت الحقيقي.
- أتمتة عملية التدقيق الداخلي (Internal Audit Automation).

المحور التاسع: البيئة التنظيمية والرقابية في المملكة العربية السعودية

- دور البنك المركزي السعودي (SAMA) في تنظيم التحول الرقمي وإدارة المخاطر.
- الإطار التنظيمي للأمن السيبراني وحوكمة البيانات في القطاع المصرفي السعودي.
- دور هيئة السوق المالية (CMA) في الرقابة على الشركات التابعة للبنوك في المجال التقني.
- مقارنة بين المعايير المحلية والمعايير الدولية في إدارة المخاطر الرقمية.
- المحور العاشر: الخاتمة

المحور الأول: الإطار المفاهيمي للمخاطر التشغيلية (Operational Risk)

المخاطر التشغيلية هي واحدة من الأنواع الثلاثة الرئيسية للمخاطر التي تواجه المؤسسات المالية (إلى جانب مخاطر الائتمان ومخاطر السوق).

1. تعريف المخاطر التشغيلية

• وفقاً للجنة بازل للرقابة المصرفية (Basel Committee):

هي خطر الخسارة الناتجة عن عدم كفاية أو فشل العمليات الداخلية أو الأفراد أو الأنظمة، أو نتيجة الأحداث الخارجية.

ويستثني هذا التعريف الخطر الاستراتيجي وخطر السمعة. ويُعد تعريف بازل هو الأكثر شيوعاً واستخداماً تنظيمياً.

• المفاهيم الأكاديمية والموسعة:

تُعرف المخاطر التشغيلية أحياناً بشكل أوسع كأي خطر غير مالي. يركز المفهوم الأكاديمي على أن هذا النوع من المخاطر ينبع من طبيعة العمليات اليومية للمؤسسة، بما في ذلك الأخطاء البشرية، والفشل التقني، وعدم الالتزام بالقوانين.

2. تصنيفات المخاطر التشغيلية

تحدد اتفاقية بازل الثانية (Basel II) أربع فئات رئيسية لمصادر المخاطر التشغيلية، والتي تنقسم إلى سبعة أنواع من الخسائر (أحداث الخسارة):

المصدر الأساسي	الفئة (Event Type)	الوصف الموجز
فشل الأفراد	الأفراد (People)	الخسائر الناتجة عن الأخطاء البشرية، الاحتيال الداخلي، الكفاءة غير الملائمة، أو نزاعات التوظيف (مثل: التمييز، التحرش، قضايا الصحة والسلامة).
فشل العمليات	العمليات (Process)	الخسائر الناتجة عن فشل تصميم المنتج، إدارة الموردين، أو التنفيذ غير السليم للصفقات والعمليات (مثل: تسوية الصفقات، الإبلاغ غير الدقيق).

فشل الأنظمة	الأنظمة (Systems)	الخسائر الناتجة عن فشل الأجهزة، البرمجيات، أو الاتصالات، بما في ذلك انقطاع الأعمال وفشل الأنظمة الأمنية.
الأحداث الخارجية	الأحداث الخارجية (External Events)	الخسائر الناتجة عن السرقة الخارجية، الاحتتيال السيبراني، الكوارث الطبيعية، أو أي إضرار من أطراف ثالثة (مثل: هجمات الهاكرز، الدعاوى القضائية ضد العميل).

3. مكونات عملية إدارة المخاطر التشغيلية

إدارة المخاطر التشغيلية هي عملية دورية ومستمرة تشمل أربع مراحل رئيسية:

1. التحديد (Identification): تحديد وتقييم المخاطر المحتملة قبل حدوث

الخسارة. يتم ذلك من خلال أدوات مثل تقييم المخاطر والتحكم الذاتي (RCSA)،

ومؤشرات المخاطر الرئيسية (KRIs)، وسجل بيانات الخسائر التشغيلية.

2. القياس (Measurement): تقدير حجم وتكرار الخسائر المحتملة باستخدام

نماذج كمية (مثل توزيعات الاحتمالية) أو تقييمات نوعية (مثل مصفوفة

المخاطر).

3. المراقبة (Monitoring): تتبع مستويات المخاطر الفعلية مقابل الحدود

الموضوعة ومؤشرات المخاطر الرئيسية (KRIs).

4. التخفيف (Mitigation) والتحكم (Control): اتخاذ الإجراءات اللازمة لتقليل

احتمالية حدوث الخسارة أو تقليل حجمها عند وقوعها. يشمل ذلك تحسين الضوابط

الداخلية، وتدريب الموظفين، وشراء التأمين.

4. مفهوم الخسائر التشغيلية وأنواعها

الخسارة التشغيلية (Operational Loss): هي أي تكلفة أو مصاريف تتكبدها

المؤسسة نتيجة لوقوع حدث خطر تشغيلي.

• الخسائر المباشرة (Direct Losses): هي الخسائر التي يمكن قياسها بشكل

مباشر وواضح مالياً وتكون مرتبطة بشكل مباشر بحدث الخسارة.

◦ أمثلة: الأموال المفقودة بسبب الاحتيال، تكلفة إصلاح نظام فاشل،

الغرامات التنظيمية المدفوعة.

• الخسائر غير المباشرة (Indirect Losses): هي الخسائر التي لا يمكن

قياسها بسهولة وتظهر في شكل تكاليف فرصة ضائعة أو تأثيرات طويلة الأجل

على الأداء التشغيلي والسمعة.

◦ أمثلة: خسارة إيرادات بسبب انقطاع النظام، انخفاض قيمة السهم بسبب

الإضرار بالسمعة، تكاليف إعادة بناء ثقة العملاء.

المحور الثاني: الإطار التنظيمي لإدارة المخاطر (لجنة بازل)

لجنة بازل للرقابة المصرفية (BCBS) هي الجهة التي تضع الإطار التنظيمي العالمي للمؤسسات المالية، وهدفها الأساسي هو تعزيز استقرار النظام المالي.

1. اتفاقيات بازل ودورها في تعزيز إدارة المخاطر التشغيلية

• بازل (2004) II: كانت نقطة التحول الأساسية لإدارة المخاطر التشغيلية.

◦ أهميتها: للمرة الأولى، أصبحت المخاطر التشغيلية تتطلب رأس مال

تنظيمي (Regulatory Capital) مقابلها (الركيزة الأولى).

◦ الهيكل: قامت على ثلاث ركائز:

1. الحد الأدنى لمتطلبات رأس المال: تحديد طرق قياس المخاطر.

2. المراجعة الإشرافية: دور الجهات التنظيمية في تقييم مدى كفاية

رأس مال البنك وإدارة مخاطره.

3. انضباط السوق: متطلبات الإفصاح والشفافية لتعزيز تقييم السوق

للمخاطر.

• بازل III (2010 وما تلاها): جاءت استجابة للأزمة المالية العالمية 2008

لتعزيز جودة ونوعية رأس المال المصرفي.

○ التأثير على المخاطر التشغيلية: لم تغير بازل III المفهوم، لكنها زادت

متطلبات رأس المال بشكل عام، وأدخلت لاحقاً (في الإصدارات النهائية)

الطريقة القياسية المبسطة (SMA) لتحل محل الطرق القديمة.

2. الطرق المعتمدة لقياس رأس المال مقابل المخاطر التشغيلية (بازل II)

كانت اتفاقية بازل II توفر ثلاثة خيارات لقياس رأس المال المطلوب مقابل المخاطر

التشغيلية (الركيزة الأولى):

الطريقة	الاسم الإنجليزي	المبدأ الأساسي	المؤسسات المستخدمة
الطريقة الأساسية للمؤشرات	Basic Indicator Approach (BIA)	تعتمد على مؤشر واحد وهو متوسط إجمالي الدخل السنوي للبنك. يتم تخصيص نسبة ثابتة (15%) من هذا الدخل كمتطلب لرأس المال التشغيلي.	البنوك الأصغر أو الأقل تعقيداً.

البنوك المتوسطة إلى الكبيرة.	يتم تقسيم العمليات المصرفية إلى خطوات عمل محددة (مثل: تمويل الشركات، التجزئة). ولكل خط عمل، يتم تطبيق نسبة مختلفة (β) من إجمالي الدخل الخاص به لحساب متطلب رأس المال.	Standardised Approach (SA)	طريقة المؤشرات القياسية
البنوك الكبيرة ذات أنظمة إدارة مخاطر متطورة.	تسمح للبنك باستخدام نماذجه الداخلية الخاصة لتقدير متطلبات رأس المال. تتطلب موافقة المشرف وتعتمد على بيانات الخسائر الداخلية والخارجية والسيناريوهات.	Advanced Measurement Approach (AMA)	طريقة القياس المتقدمة

• ملاحظة (بازل III): استبدلت بازل III الطريقتين BIA و AMA بطريقة جديدة

موحدة هي الطريقة القياسية المبسطة (Standardised Measurement)

(SMA – Approach)، وهي تجمع بين عناصر من الطرق السابقة وتعتمد

على مؤشر الأعمال (Business Indicator) ومركب الخسارة الداخلية.

3. متطلبات الحوكمة والضوابط الداخلية في ضوء إرشادات بازل

تركز إرشادات بازل (الركيزة الثانية) بشدة على الحوكمة وإطار الرقابة:

1. مجلس الإدارة والإدارة العليا: يجب أن يكون مجلس الإدارة مسؤولاً عن تحديد

استراتيجية المخاطر والموافقة على إطار إدارة المخاطر.

2. الضوابط الداخلية: يجب تطبيق ضوابط داخلية فعالة في جميع مستويات المؤسسة

لتقليل المخاطر التشغيلية.

3. نموذج خطوط الدفاع الثلاثة (Three Lines of Defense Model):

◦ الدفاع الأول: وحدات الأعمال والعمليات (تملك المخاطر وتديرها يومياً).

◦ الدفاع الثاني: وظائف إدارة المخاطر والامتثال (تضع الإطار وتراقب

حدود المخاطر).

◦ الدفاع الثالث: التدقيق الداخلي (يوفر تأكيداً مستقلاً بأن الإطار يعمل

بفعالية).

المحور الثالث: مفاهيم ونماذج التحول الرقمي (Digital Transformation)

التحول الرقمي يمثل التحدي الأكبر والفرصة الأعظم للمؤسسات المالية في العصر الحالي.

1. التعريف الشامل للتحول الرقمي وخصائصه في القطاع المالي

التحول الرقمي (Digital Transformation – DX): هو عملية استراتيجية وثقافية وتنظيمية شاملة لاستخدام التكنولوجيات الرقمية لإعادة تصميم نماذج الأعمال، والعمليات، والثقافة التنظيمية، وتجارب العملاء، بهدف خلق قيمة جديدة أو تحسين الكفاءة بشكل جذري.

خصائصه في القطاع المالي:

- **التركيز على العميل:** استخدام البيانات والذكاء الاصطناعي لفهم احتياجات العميل وتخصيص الخدمات (Hyper-personalization).
- **الكفاءة التشغيلية:** أتمتة العمليات الخلفية (Back-office) لخفض التكلفة وتقليل المخاطر التشغيلية.
- **الابتكار في المنتجات:** تقديم خدمات جديدة تماماً (مثل المحافظ الرقمية، التمويل اللامركزي).
- **المرونة (Agility):** تبني منهجيات العمل السريع (Agile) والمنصات المفتوحة للتكيف مع المتغيرات السوقية.

2. مقارنة بين الرقمنة، والأتمتة، والتحول الرقمي

هذه المصطلحات مترابطة، لكنها تمثل مستويات مختلفة من التغيير:

المفهوم	التعريف	الهدف
الرقمنة (Digitization)	تحويل المعلومات من الشكل التناظري (Analog) إلى الشكل الرقمي (Digital).	تحسين كفاءة تخزين واسترجاع البيانات.
الأتمتة (Automation)	استخدام التكنولوجيا لتنفيذ مهام أو عمليات متكررة كانت تتم سابقاً يدوياً (مثل روبوتات الأتمتة الروبوتية RPA).	زيادة سرعة ودقة وكفاءة العملية المحددة.
التحول الرقمي (Digital Transformation)	التغيير الشامل لنموذج العمل وهيكل المؤسسة وثقافتها عبر تبني التكنولوجيا.	خلق قيمة جديدة وإعادة تعريف علاقات العمل والعملاء.

3. الركائز التكنولوجية للتحول الرقمي

يعتمد التحول الرقمي على دمج مجموعة من التقنيات المتقدمة:

- **الذكاء الاصطناعي والتعلم الآلي (AI/ML):** يُستخدم في تقييم المخاطر (مخاطر الائتمان والاحتيال)، تخصيص المنتجات، وأتمتة اتخاذ القرارات.
- **الحوسبة السحابية (Cloud Computing):** توفير المرونة وقابلية التوسع وخفض تكاليف البنية التحتية. تسمح بإطلاق منتجات وخدمات جديدة بسرعة.
- **البيانات الضخمة والتحليلات (Analytics & Big Data):** جمع وتحليل كميات هائلة من البيانات الداخلية والخارجية لاستخلاص رؤى استراتيجية حول سلوك العملاء والمخاطر.
- **سلسلة الكتل (Blockchain):** تستخدم في تطبيقات التسوية والمدفوعات الآمنة والشفافة (خاصة في التمويل التجاري).

4. نماذج تبني التحول الرقمي في المؤسسات المالية

تتبنى المؤسسات المالية عادةً أحد النماذج التالية أو مزيجاً منها:

1. النموذج المتدرج (Phased/Incremental Model): البدء بأتمتة ورقمنة

العمليات الأكثر إلحاحاً أو الأسهل تنفيذاً، ثم التوسع تدريجياً ليشمل إعادة تصميم الخدمات الأساسية.

2. نموذج الكيان المنفصل (Separate Digital Unit/Subsidiary): إنشاء

وحدة عمل رقمية جديدة بالكامل أو بنك رقمي تابع يعمل بمنأى عن الهياكل القديمة، مما يسمح بالتحرك من الإجراءات والأنظمة القديمة والابتكار السريع.

3. نموذج الشراكة (Partnership Model): التعاون مع شركات التكنولوجيا

المالية (FinTechs) لدمج حلولها المبتكرة في منظومة البنك الداخلية، مما يسرع من وقت الوصول إلى السوق (Time-to-Market).

4. نموذج التركيز على العميل (Customer-Centric Model): يبدأ التحول من

تحسين نقاط الاتصال الرقمية للعميل (تطبيقات الموبايل، الخدمات المصرفية عبر الإنترنت)، ثم يتوسع تدريجياً ليشمل تحديث الأنظمة الداخلية الداعمة.

المحور الرابع: تطبيقات التحول الرقمي في العمليات المصرفية

يُعد القطاع المصرفي من أكثر القطاعات استفادة من الابتكار التكنولوجي، حيث تعيد التقنيات الحديثة تشكيل العمليات الأساسية من الواجهة الأمامية (Front Office) إلى العمليات الخلفية (Back Office).

1. استخدام الذكاء الاصطناعي (AI) في أتمتة العمليات الأساسية

• التعرف على العملاء (KYC) وعمليات فتح الحسابات: تستخدم نماذج الذكاء

الاصطناعي لتحليل الوثائق البيومترية وصور الهوية، مما يسرع عملية التحقق من

الهوية (e-KYC) ويقلل الأخطاء البشرية والوقت اللازم للامتثال.

• معالجة القروض والائتمان: تعتمد خوارزميات التعلم الآلي على تحليل مجموعات

بيانات ضخمة لتقييم الجدارة الائتمانية بشكل أسرع وأكثر دقة من النماذج

الإحصائية التقليدية، مما يقلل مخاطر الائتمان والأخطاء التشغيلية في مرحلة

التقييم.

• مكافحة الاحتيال وغسل الأموال (AML/Fraud Detection): يراقب الذكاء

الاصطناعي المعاملات في الوقت الفعلي لتحديد الأنماط الشاذة أو السلوكيات

المشبوهة بدقة عالية جداً، متفوقاً على أنظمة الكشف القائمة على القواعد الثابتة.

2. دور البيانات الضخمة (Big Data Analytics) في اتخاذ القرارات

• تحسين تجربة العميل (CX): يتيح تحليل البيانات الضخمة للمؤسسات المصرفية

فهم سلوك العميل وتفضيلاته (مثل عادات الإنفاق)، مما يمكنها من تقديم عروض

وخدمات مالية مخصصة وفائقة الاستهداف (Hyper-personalization).

• اتخاذ القرارات الاستراتيجية والمخاطر: توفير رؤى حول السوق، وتحديد المخاطر

الناشئة (مثل التغيرات في أنماط السداد على مستوى محفظة كاملة)، والمساعدة

في تحديد التسعير الأمثل للمنتجات.

3. تأثير تقنية البلوك تشين (Blockchain)

تستخدم تقنية السجلات الموزعة (DLT) والبلوك تشين لزيادة الشفافية والأمان في

المعاملات، خصوصاً في:

- كفاءة وتسوية المدفوعات عبر الحدود: تقلل البلوك تشين من عدد الوسطاء المطلوبين لتسوية المدفوعات الدولية، مما يخفض التكلفة والوقت، ويزيد الشفافية، ويقلل مخاطر التسوية (Settlement Risk).
- التمويل التجاري (Trade Finance): تساعد في رقمنة المستندات التجارية وإنشاء سجل غير قابل للتغيير للمعاملات، مما يقلل الاحتيال الوثائقي ويسرع عملية التمويل.

4. تحول قنوات الخدمة

شهدت القنوات المصرفية تحولاً جذرياً من الاعتماد على الأماكن المادية إلى المنصات الرقمية:

- المنصات الرقمية أولاً (Digital-First): أصبحت تطبيقات الهاتف المحمول والمواقع الإلكترونية هي القنوات الرئيسية لتقديم معظم الخدمات المصرفية.
- فروع المستقبل (Future Branches): تحول دور الفرع التقليدي من مركز للمعاملات إلى مركز استشاري ومبيعات متخصص للقروض والخدمات المعقدة.
- الواجهات المفتوحة (Open APIs): استخدام واجهات برمجة التطبيقات المفتوحة للسماح بالتعاون مع شركات الطرف الثالث (FinTechs) وتقديم خدمات مالية مدمجة (Embedded Finance).

المحور الخامس: الأثر المزدوج للتحويل الرقمي على المخاطر التشغيلية

التحول الرقمي سلاح ذو حدين بالنسبة للمخاطر التشغيلية؛ فهو يحل المشكلات التقليدية ولكنه يخلق تحديات جديدة.

1. الأثر الإيجابي (تقليل المخاطر التشغيلية التقليدية)

المجال	الأثر الإيجابي للرقمنة	المخاطر التقليدية التي يتم تخفيفها
الأتمتة	إلغاء التدخل البشري في المهام المتكررة.	الأخطاء البشرية، سهو الموظفين، أخطاء إدخال البيانات.
البيانات والتحليل	توحيد مصادر البيانات وتحسين جودة التقارير.	سوء اتخاذ القرار، التقارير غير الدقيقة، تضارب البيانات.
التصميم الرقمي	تبسيط رحلة العميل وتقليل خطوات العملية.	فشل العمليات غير الكفؤة، زمن المعالجة الطويل، الفشل في الالتزام.

الامتثال	الأتمتة الروبوتية (RPA) لتنفيذ متطلبات الامتثال والتدقيق.	مخاطر الامتثال، الغرامات التنظيمية.
----------	---	--

2. الأثر السلبي (المخاطر المستحدثة)

يؤدي التعقيد التكنولوجي إلى ظهور فئة جديدة من المخاطر التشغيلية:

- **مخاطر النماذج (Model Risk):** الاعتماد المفرط على خوارزميات الذكاء الاصطناعي ونماذج التعلم الآلي. يمكن أن تؤدي النماذج غير المدربة جيداً أو المتحيزة إلى قرارات خاطئة (مثل رفض قروض لأسباب غير عادلة أو فشل في تحديد الاحتيال الجديد).
- **مخاطر الطرف الثالث (Third-Party Risk):** زيادة الاعتماد على مقدمي الخدمات السحابية الخارجيين (Cloud Providers) أو شركات التكنولوجيا المالية، مما ينقل جزءاً من المخاطر التشغيلية إلى كيانات خارجية يصعب التحكم فيها.
- **مخاطر أمن البيانات والخصوصية:** زيادة كمية البيانات الحساسة المخزنة رقمياً يجعل المؤسسة هدفاً أكبر للهجمات السيبرانية وانتهاكات قوانين حماية البيانات (مثل GDPR).

• مخاطر البنية القديمة (Legacy Risk): دمج التقنيات الجديدة مع الأنظمة

القديمة (التي تعمل لعقود) يخلق نقاط ضعف ونقاط فشل جديدة.

3. التحليل المقارن بين المخاطر التشغيلية التقليدية والرقمية

الخاصية	المخاطر التشغيلية التقليدية	المخاطر التشغيلية في البيئة الرقمية
المصدر الرئيسي	الأفراد، العمليات اليدوية، الأخطاء المادية.	الأنظمة التكنولوجية، الأمن السيبراني، النماذج والخوارزميات.
القياس	سهل القياس (سجلات الخسائر التاريخية).	صعب القياس والتنبؤ (أحداث نادرة ذات تأثير هائل).
الانتشار والتأثير	محلي ومحدود (خطأ في فرع أو عملية).	عالمي وفوري (فشل خوارزمي يؤثر على ملايين المعاملات).
آلية التخفيف	الضوابط الداخلية، التدريب، الفصل بين المهام.	الرقابة على النماذج، أمن المعلومات، خطط التعافي من الكوارث.

المحور السادس: إدارة المخاطر السيبرانية ومخاطر تقنية المعلومات

تُعد المخاطر السيبرانية (Cyber Risk) أحد أهم أنواع المخاطر التشغيلية في العصر الرقمي، نظراً لاعتماد البنوك الكلي على الأنظمة الإلكترونية.

1. تعريف المخاطر السيبرانية ومصادرها في البنوك

• **المخاطر السيبرانية:** هي خطر الخسارة المالية، أو تعطيل العمليات، أو الإضرار

بالسمعة الناتج عن فشل أنظمة المعلومات أو البنية التحتية التكنولوجية، أو

اختراقها بشكل متعمد أو غير متعمد.

• **المصادر الرئيسية في البنوك:**

◦ **الجهات الفاعلة الخبيثة (Malicious Actors):** مجرمو الإنترنت،

قراصنة برعاية دول، موظفون ساخطون (Threat Actors).

◦ **نقاط الضعف التكنولوجية:** الثغرات الأمنية في البرامج، الإعدادات الخاطئة

لجدران الحماية، الأنظمة القديمة غير المحدثة.

◦ **الهندسة الاجتماعية:** هجمات التصيد الاحتيالي (Phishing) التي

تستهدف الموظفين كأضعف حلقة في السلسلة الأمنية.

◦ **الفشل الداخلي غير المتعمد:** الأخطاء البشرية في تشغيل الأنظمة أو

تحديثها.

2. مخاطر استمرارية الأعمال (BCR) والتعافي من الكوارث (DR)

في البيئة الرقمية، يعني فشل النظام توقف البنك عن العمل:

• **خطر استمرارية الأعمال:** خطر تعرض البنك لتوقف كبير في خدماته نتيجة لأي

حدث (كارثة طبيعية، هجوم سيبراني، فشل تقني كبير).

• **التعافي من الكوارث:** الإجراءات والخطط اللازمة لاستعادة البنية التحتية

التكنولوجية والوصول إلى البيانات والأنظمة الحيوية في غضون فترة زمنية محددة

مسبقاً بعد وقوع كارثة.

◦ المقاييس الرئيسية: الحد الأقصى لزمان الانقطاع المقبول (MTPD)،

وهدف نقطة التعافي (RPO)، وهدف زمن التعافي (RTO).

3. مخاطر البنية التحتية التكنولوجية وفشل الأنظمة

تشمل المخاطر التي تنبع من البنية التحتية الصلبة والبرمجية نفسها:

• **فشل الأجهزة (Hardware Failure):** تعطل الخوادم أو شبكات التخزين.

• **فشل البرمجيات (Software Failure):** وجود أخطاء برمجية (Bugs) أو فشل

في التكامل بين الأنظمة المختلفة.

• **مخاطر السعة (Capacity Risk):** عدم قدرة البنية التحتية على التعامل مع

حجم متزايد من المعاملات الرقمية (مثل ذروة المعاملات في نهاية الشهر).

4. استراتيجيات التخفيف من المخاطر السيبرانية

تتطلب إدارة المخاطر السيبرانية نهجاً متعدد الأبعاد:

1. **الحوكمة الأمنية:** تحديد مسؤوليات واضحة للأمن السيبراني على مستوى مجلس

الإدارة والإدارة العليا.

2. **ضوابط الوصول:** تطبيق مبدأ الحد الأدنى من الامتيازات (Least Privilege)

والتحقق متعدد العوامل (MFA) لتقييد وصول الموظفين إلى الأنظمة الحساسة.

3. **الكشف والاستجابة:** الاستثمار في أنظمة مراقبة الأمن في الوقت الفعلي (SIEM)

وفرق الاستجابة للحوادث (Incident Response Teams) لتقليل زمن

اكتشاف الاختراق والاستجابة له.

4. **التدريب والوعي:** التدريب المستمر للموظفين لرفع مستوى الوعي بمخاطر التصيد

الاحتمالي والتهديدات الهندسية الاجتماعية.

5. **اختبار الاختراق:** إجراء اختبارات اختراق منتظمة (Penetration Testing)

وتقييمات للثغرات الأمنية لتحديد نقاط الضعف قبل استغلالها من قبل المهاجمين.

6. **أمن الطرف الثالث:** وضع ضوابط صارمة على الموردين الخارجيين والتأكد من

توافق مستوياتهم الأمنية مع معايير البنك.

تحليل متقدم لإدارة المخاطر التشغيلية في العصر الرقمي

المحور السابع: مخاطر الطرف الثالث (Third-Party Risk) والشركات التقنية المالية (FinTech)

في ظل التحول الرقمي، زاد اعتماد البنوك على شركاء خارجيين لتقديم الخدمات التكنولوجية (مثل الحوسبة السحابية، تطوير التطبيقات)، مما نقل جزءاً من المخاطر التشغيلية إلى هذه الأطراف.

1. مفهوم مخاطر الطرف الثالث وأهميته

- **مفهوم مخاطر الطرف الثالث:** هو خطر التعرض لخسارة مالية، أو ضرر في السمعة، أو عدم امتثال ناتج عن فشل الموردين الخارجيين أو الشركاء أو المقاولين في تقديم الخدمات المتفق عليها أو عدم التزامهم بالمعايير الأمنية والتنظيمية.
- **الأهمية في ظل الحوسبة السحابية والـ FinTech:** تعتمد البنوك بشكل متزايد على البنية التحتية السحابية (PaaS, IaaS, SaaS) لتقديم خدماتها، كما تتعاون مع شركات التكنولوجيا المالية (FinTech) لتقديم حلول مبتكرة. أي فشل أو اختراق لدى هؤلاء الشركاء ينعكس مباشرة على البنك نفسه.

2. إدارة مخاطر سلسلة التوريد التكنولوجية والمقاولين الخارجيين

تتطلب إدارة هذه المخاطر دورة حياة متكاملة:

1. **العناية الواجبة الأولية (Due Diligence):** قبل التعاقد، يجب تقييم الوضع

المالي للمورد، قدرته التشغيلية، بيئته الأمنية، وخطط استمرارية أعماله (BCP)

للتأكد من توافقه مع معايير البنك.

2. **التعاقد:** يجب أن تتضمن العقود بنوداً واضحة بشأن مستويات الخدمة (SLAs)،

حقوق التدقيق، والمسؤوليات الأمنية والقانونية في حال وقوع اختراق أو فشل.

3. **المراقبة المستمرة (Ongoing Monitoring):** لا تكفي المراجعات السنوية.

يجب مراقبة أداء الموردين، وضعهم الأمني، وتغييراتهم التنظيمية بشكل مستمر

(على سبيل المثال، عبر منصات مراقبة المخاطر الآلية).

4. **إدارة الخروج (Exit Strategy):** يجب وجود خطة واضحة وموثقة للانسحاب

من علاقة التعاقد (سواء انتهاء العقد أو إنهائه مبكراً) تضمن نقل البيانات

والخدمات بسلاسة وأمان إلى بديل دون انقطاع للعمل.

3. **آليات تقييم ومراقبة الالتزام التنظيمي للشركات التكنولوجية**

تتضمن الآليات التنظيمية ما يلي:

• **ضوابط الامتثال:** التأكد من التزام الموردين باللوائح المحلية والدولية (مثل لوائح

حماية البيانات، ومتطلبات بازل).

• **حقوق التدقيق (Right to Audit):** يجب أن يحتفظ البنك بحق تدقيق أنظمة

المورد ومراجعة ضوابطه الأمنية والتشغيلية بشكل دوري.

• **الشهادات القياسية:** طلب شهادات أمنية معترف بها دولياً من الموردين (مثل

ISO 27001، SOC 2 Type II).

• **تقارير التقييم:** الاعتماد على تقارير تقييم الأمن السيبراني المستقلة التي تُظهر

نقاط القوة والضعف لدى المورد.

المحور الثامن: توظيف التقنيات الرقمية في تعزيز فاعلية ORM (إدارة المخاطر

التشغيلية)

تُعد التكنولوجيا الرقمية الأداة الأكثر فعالية لـ "رقمنة" وتحسين وظيفة إدارة المخاطر

التشغيلية (ORM) نفسها.

1. دور الذكاء الاصطناعي في المراقبة واكتشاف الاحتيال والشذوذ

• **المراقبة الآلية (Automated Monitoring):** يستخدم الذكاء الاصطناعي

لتحليل سجلات النظام (Logs) وأنماط المعاملات على مدار الساعة لاكتشاف

أي سلوك تشغيلي غير متوقع أو مخالف للضوابط المعيارية.

• **اكتشاف الشذوذ (Anomaly Detection):** بدلاً من البحث عن أنماط احتيال

معروفة، يمكن للنماذج أن تتعرف على الانحرافات الدقيقة عن سلوك العميل أو

الموظف المعتاد (مثل وصول موظف إلى نظام غير معتاد في وقت غير

اعتيادي)، مما يكشف عن التهديدات الداخلية أو الهجمات الجديدة.

2. استخدام التعلم الآلي في بناء نماذج قياس وتوقع الخسائر

• **توقع الخسائر (Loss Prediction):** يمكن للتعلم الآلي (ML) بناء نماذج

إحصائية أكثر تعقيداً ودقة من النماذج التقليدية لتوقع حجم وتكرار الخسائر

التشغيلية المحتملة، بالاستناد إلى مجموعات واسعة من البيانات التاريخية،

ومؤشرات المخاطر، وخصائص خطوط العمل.

• **تحسين تخصيص رأس المال:** تُمكن دقة التوقع العالية البنوك من تخصيص رأس

المال التنظيمي والاقتصادي بشكل أكثر كفاءة ضد المخاطر التشغيلية.

3. الاستفادة من تحليلات البيانات الضخمة لتحديد مؤشرات المخاطر الرئيسية (KRIs)

• **KRIs في الوقت الحقيقي:** تتيح تحليلات البيانات الضخمة مراقبة آلاف مؤشرات

المخاطر (KRIs) بشكل مستمر (مثل: عدد فشل تسجيل الدخول، زمن استجابة

النظام، حجم شكاوى العملاء) وتحديد الاتجاهات والمشكلات قبل أن تتحول إلى

خسائر فعلية.

• **التحليل السببي (Root Cause Analysis):** يمكن للتحليلات المتقدمة أن

تربط بين مؤشرات الأداء التشغيلي ومؤشرات المخاطر، مما يساعد في تحديد

الأسباب الجذرية لأحداث الخسارة.

4. أتمتة عملية التدقيق الداخلي (Internal Audit Automation)

- **التدقيق المستمر (Continuous Auditing):** استخدام أدوات الأتمتة والذكاء

الاصطناعي لإجراء فحوصات تدقيقية منتظمة ومستمرة لضمان الامتثال للسياسات واللوائح، بدلاً من الاعتماد على التدقيق الدوري.

- **التدقيق الموجه بالمخاطر:** يمكن للذكاء الاصطناعي تحديد المناطق التي تحمل

أعلى مخاطر تشغيلية ليتم توجيه جهود فرق التدقيق إليها، مما يزيد من كفاءة عملية التدقيق.

المحور التاسع: البيئة التنظيمية والرقابية في المملكة العربية السعودية

يتمتع القطاع المالي في المملكة العربية السعودية بإطار تنظيمي متقدم يهدف إلى دعم التحول الرقمي مع الحفاظ على الاستقرار المالي والأمني.

1. دور البنك المركزي السعودي (SAMA)

- **تنظيم التحول الرقمي:** يقود البنك المركزي السعودي مبادرات مثل البنوك الرقمية

وتكنولوجيا الـ FinTech، ويضع الإطار التنظيمي لها لضمان نمو القطاع مع حماية مصالح العملاء.

- **إدارة المخاطر:** يفرض SAMA لوائح صارمة على المؤسسات المالية بشأن إدارة

المخاطر التشغيلية والسيبرانية، متطلباً بناء أطر قوية للحوكمة والضوابط الداخلية تتوافق مع معايير بازل.

2. الإطار التنظيمي للأمن السيبراني وحوكمة البيانات

- **إطار الأمن السيبراني:** أصدر SAMA إطاراً شاملاً للأمن السيبراني (Cyber Security Framework) والذي أصبح إلزامياً على جميع المؤسسات الخاضعة لإشرافه. يحدد هذا الإطار المتطلبات الدنيا للضوابط الأمنية وإدارة الهجمات السيبرانية.
- **حوكمة البيانات:** وضع متطلبات صارمة لحوكمة البيانات وحمايتها، بما في ذلك تحديد مكان تخزين البيانات (عادة داخل المملكة) والضوابط على نقل البيانات عبر الحدود، لضمان خصوصية معلومات العملاء.

3. دور هيئة السوق المالية (CMA)

- **الرقابة على الشركات التقنية:** على الرغم من أن SAMA يشرف على البنوك، تلعب هيئة السوق المالية (CMA) دوراً رقابياً على شركات التكنولوجيا التابعة للبنوك، وعلى الشركات المالية المدرجة والكيانات التي تقدم خدمات تقنية مرتبطة بالاستثمار والأوراق المالية، لضمان الامتثال وحماية المستثمرين.

4. مقارنة بين المعايير المحلية والمعايير الدولية

المعايير المحلية (SAMA)	المعايير الدولية (بازل)، (ISO)	الخاصية

الأساس	مبادئ وإرشادات عامة.	لوائح ملزمة ومفصلة.
الأمن السيبراني	متطلبات عامة (FSSCC).	إطار أمني محدد وخاص بـ SAMA (SAMA CSF).
الحوسبة السحابية	إرشادات عامة لإدارة مخاطر الطرف الثالث.	متطلبات مفصلة لمقدمي الخدمات السحابية.
الهدف	الاستقرار المالي العالمي.	الاستقرار المالي وحماية العملاء محلياً.

• الخلاصة: تعتمد المعايير المحلية السعودية بشكل كبير على إرشادات بازل و

ISO، ولكنها تضيف طبقات إلزامية وتفصيلية للمتطلبات، خاصة فيما يتعلق

بالأمن السيبراني وحوكمة البيانات، لتتناسب البيئة التشغيلية المحلية.

المحور العاشر: الخاتمة

يُعد التفاعل بين التحول الرقمي والمخاطر التشغيلية محركاً رئيسياً للابتكار والتنظيم في القطاع المصرفي. بينما يوفر التحول الرقمي أدوات قوية لتقليل الأخطاء البشرية وتحسين الكفاءة، فإنه يقدم في الوقت نفسه تحديات جديدة ومعقدة مثل المخاطر السيبرانية ومخاطر الطرف الثالث. النجاح في العصر الرقمي يتطلب من المؤسسات المالية ليس فقط تبني التكنولوجيا، بل أيضاً دمج إدارة المخاطر (خاصةً المخاطر التشغيلية والسيبرانية) في صميم استراتيجيتها التشغيلية، بما يتوافق مع الأطر التنظيمية القوية محلياً (مثل إطار SAMA) وعالمياً (بازل). هذا التكامل يضمن نمواً مستداماً ومرونة أكبر في مواجهة التهديدات المتطورة.

الفصل الثالث

الفصل الثالث: منهجية الدراسة وإجراءاتها

1. منهج الدراسة (Research Methodology)

لتحقيق أهداف الدراسة والإجابة على تساؤلاتها، اعتمدت الدراسة على **المنهج الوصفي**

التحليلي (Descriptive Analytical Approach).

• **وصف المنهج:** يقوم هذا المنهج على وصف الظاهرة أو المشكلة محل الدراسة

(أثر التحول الرقمي على إدارة المخاطر التشغيلية) كما هي قائمة في الواقع، ثم

جمع البيانات والمعلومات المتعلقة بها، وتحليل هذه البيانات إحصائياً (عبر تحليل

الانحدار والارتباط) لاستخلاص العلاقات والنتائج، ومن ثم اختبار الفرضيات

وإصدار التوصيات المناسبة.

• **ملائمة المنهج:** يُعد المنهج الوصفي التحليلي هو الأنسب لهذا النوع من الدراسات

الميدانية، حيث يتطلب تحديد مستوى التبني الرقمي (المتغير المستقل) وتقييم

فاعلية إدارة المخاطر (المتغير التابع) في البنوك السعودية القائمة.

2. مجتمع الدراسة وعينتها

أ. مجتمع الدراسة (Population)

يتكون مجتمع الدراسة من جميع الأفراد العاملين في المستويات الإدارية المتخصصة

والذين لديهم ارتباط مباشر بـ "العمليات المصرفية" و "إدارة المخاطر التشغيلية" و "التحول

الرقمي" في البنوك التجارية العاملة في المملكة العربية السعودية.

ويشمل هذا:

1. مديري ورؤساء أقسام إدارة المخاطر التشغيلية (Operational Risk).
2. الموظفين المتخصصين في الامتثال (Compliance) والتدقيق الداخلي (Internal Audit).
3. مديري ورؤساء أقسام تقنية المعلومات والتحول الرقمي.
4. مديري العمليات المصرفية (Banking Operations) الذين يشرفون على القنوات الرقمية.

ب. عينة الدراسة (Sample)

- نظراً لصعوبة الوصول إلى كامل مجتمع الدراسة، ستعتمد الدراسة على **عينة قصدية** (Purposive Sample) من الكوادر القيادية والتخصصية في البنوك السعودية. سيتم اختيار الأفراد بعناية لضمان أنهم يمتلكون المعرفة والخبرة اللازمة للإجابة على محاور الاستبيان المتعلقة بتقنيات التحول الرقمي وإجراءات إدارة المخاطر.
- **حجم العينة المقترح:** يُقترح أن يتراوح حجم العينة بين (150-200) فرد، مع التركيز على البنوك الرائدة التي لديها تطبيقات متقدمة للتحول الرقمي.

• آلية التوزيع: يتم توزيع الاستبيان إلكترونياً (باستخدام أدوات مثل Google

Forms أو SurveyMonkey) لضمان سهولة الوصول إلى المشاركين في

المواقع الجغرافية المختلفة.

3. أداة الدراسة: الاستبيان (Questionnaire)

تُعد أداة جمع البيانات الرئيسية في هذه الدراسة هي الاستبيان، والذي تم تصميمه لجمع

البيانات الأولية حول متغيرات الدراسة.

تصميم الاستبيان وهيكله

ينقسم الاستبيان إلى ثلاثة أجزاء رئيسية:

الجزء الأول: البيانات الأولية والديموغرافية

يشمل معلومات حول المستجيبين مثل: المسمى الوظيفي، الخبرة، المستوى التعليمي، ونوع

البنك (إن أمكن).

الجزء الثاني: محاور قياس المتغير المستقل (التحول الرقمي)

يهدف هذا المحور إلى قياس مستوى تبني وتطبيق أدوات التحول الرقمي في البنوك

السعودية، ويتضمن عبارات تقيس الأبعاد التالية:

• تبني تقنيات الذكاء الاصطناعي (AI) والتعلم الآلي (ML).

• استخدام الحوسبة السحابية (Cloud Computing).

• الاعتماد على تحليلات البيانات الضخمة (Big Data Analytics).

الجزء الثالث: محاور قياس المتغير التابع (فاعلية إدارة المخاطر التشغيلية)

يهدف هذا المحور إلى قياس فاعلية إدارة المخاطر التشغيلية في ظل التحول الرقمي،

ويتضمن عبارات تقيس الأبعاد التالية:

• كفاءة الضوابط التشغيلية والرقابة الداخلية.

• الاستجابة للمخاطر المستحدثة (الأمن السيبراني، مخاطر الطرف الثالث).

• دقة قياس وتوقع الخسائر التشغيلية.

مقياس الإجابة

سيتم استخدام مقياس ليكرت الخماسي (Five-point Likert Scale) للإجابة على

عبارات الاستبيان، لتمكين المستجيب من التعبير عن درجة موافقه أو عدم موافقه، على

النحو التالي:

1 = أوافق بشدة (Strongly Agree)

2 = أوافق (Agree)

3 = محايد (Neutral)

4 = لا أوافق (Disagree)

5 = لا أوافق بشدة (Strongly Disagree)

الخصائص السيكومترية للأداة (Psychometric Properties)

قبل البدء بالتطبيق الفعلي للدراسة، يجب التأكد من صدق وثبات أداة الدراسة:

• الصدق (Validity): يتم التحقق منه من خلال:

◦ الصدق الظاهري (Face Validity): عرض الاستبيان في صورته الأولية

على مجموعة من المحكمين (الخبراء والأكاديميين في المجال المصرفي

وإدارة المخاطر) للتأكد من وضوح العبارات وملاءمتها للمحاور.

◦ صدق الاتساق الداخلي (Internal Consistency Validity): قياس

معامل الارتباط بين كل عبارة والمحور الذي تنتمي إليه.

• الثبات (Reliability): يتم التحقق منه من خلال تطبيق اختبار ألفا كرونباخ

(Cronbach's Alpha) للتأكد من أن الاستبيان سيعطي نفس النتائج تقريباً إذا

أعيد تطبيقه تحت نفس الظروف. يجب أن يكون معامل ألفا كرونباخ للمحاور

ككل مقبولاً (عادةً أعلى من 0.70).

4. المعالجة الإحصائية للبيانات

سيتم تحليل البيانات المجمعة باستخدام برنامج الحزم الإحصائية للعلوم الاجتماعية (SPSS)، وتتضمن المعالجة الإحصائية ما يلي:

1. **الإحصاء الوصفي:** استخدام التكرارات، النسب المئوية، المتوسطات الحسابية، والانحرافات المعيارية لوصف خصائص عينة الدراسة والإجابة على التساؤلات الوصفية.

2. **الإحصاء الاستدلالي واختبار الفرضيات:** استخدام الاختبارات الإحصائية المتقدمة مثل:

○ اختبار تحليل الانحدار المتعدد (Multiple Regression)

(Analysis): لتحديد الأثر (الإيجابي والسلبي) للمتغير المستقل (أبعاد

التحول الرقمي) على المتغير التابع (فاعلية إدارة المخاطر التشغيلية).

○ معامل الارتباط (Correlation Coefficient): لقياس قوة ونوع العلاقة

بين متغيرات الدراسة.

○ اختبار (T-test) و (ANOVA): للمقارنة بين متوسطات استجابات

العينة وفقاً لمتغيراتهم الديموغرافية (مثل الخبرة والمسمى الوظيفي).

حدود الدراسة (Study Scope and Limitations)

1. الحدود الموضوعية (Thematic Scope)

تتخصص الدراسة في قياس وتحليل الأثر المتبادل بين التحول الرقمي (كالمُتغير المستقل) وإدارة المخاطر التشغيلية (كالمُتغير التابع)، دون التعمق في أنواع المخاطر الأخرى (مثل مخاطر الائتمان أو مخاطر السوق).

2. الحدود المكانية (Geographical Scope)

تقتصر الدراسة الميدانية على البنوك التجارية العاملة داخل المملكة العربية السعودية فقط.

3. الحدود البشرية (Human Scope)

تستهدف الدراسة عينة قصدية من الكوادر الإدارية والمتخصصة العاملة في ثلاثة أقسام رئيسية داخل البنوك: إدارة المخاطر، العمليات المصرفية، والتحول الرقمي/تقنية المعلومات.

4. الحدود الزمانية (Temporal Scope)

تغطي الدراسة الفترة الزمنية التي تم فيها جمع وتحليل البيانات (الفترة من عام 2024 إلى 2025)، وتركز على تقييم الوضع الراهن لتأثير أدوات التحول الرقمي المطبقة خلال الأعوام الخمسة الماضية.

هيكل وأسئلة الاستبيان

الهدف العام للاستبيان

الهدف من هذا الاستبيان هو جمع بيانات أولية لتقييم مدى تبني البنوك السعودية لأدوات التحول الرقمي وتحديد الأثر الناتج عن هذا التبني على فاعلية وكفاءة إدارة المخاطر التشغيلية لديها.

مقياس الإجابة

سيتم استخدام مقياس ليكرت الخماسي لجميع عبارات محاور الدراسة، حيث تكون الخيارات هي:

1 = أوافق بشدة (Strongly Agree)

2 = أوافق (Agree)

3 = محايد (Neutral)

4 = لا أوافق (Disagree)

5 = لا أوافق بشدة (Strongly Disagree)

أولاً: البيانات الديموغرافية (التعريفية)

(تُصاغ كخيارات متعددة بسيطة أو إجابة مفتوحة قصيرة)

1. المسمى الوظيفي: (مدير إدارة، رئيس قسم، موظف متخصص، إلخ)
 2. سنوات الخبرة الإجمالية في القطاع المصرفي: (أقل من 5 سنوات، 5-10 سنوات، 10 سنوات فأكثر)
 3. الإدارة التي تنتمي إليها: (إدارة المخاطر، العمليات المصرفية، تقنية المعلومات/التحول الرقمي، التدقيق والامتثال)
 4. المستوى التعليمي: (بكالوريوس، ماجستير، دكتوراه)
- ثانياً: محور قياس المتغير المستقل: التحول الرقمي (4 عبارات مقترحة)
- (يهدف إلى قياس مستوى تبني التقنيات الرقمية المتقدمة في العمليات المصرفية)

رقم	العبرة
1.	يعتمد البنك على أنظمة الذكاء الاصطناعي (AI) في أتمتة الإجراءات التشغيلية الأساسية (مثل مطابقة المستندات).
2.	تُستخدم تحليلات البيانات الضخمة (Big Data Analytics) بشكل فعال للتنبؤ بالخسائر التشغيلية المحتملة.
3.	تم نقل معظم الأنظمة المصرفية الأساسية في البنك إلى بيئة الحوسبة السحابية (Cloud Computing).

4.	يساهم التبني الرقمي في تقليل الاعتماد على التدخل البشري وبالتالي يحد من الأخطاء التشغيلية اليدوية.
----	--

ثالثاً: محور قياس المتغير التابع: فاعلية إدارة المخاطر التشغيلية (4 عبارات مقترحة)

(يهدف إلى قياس كفاءة إدارة المخاطر في البيئة الرقمية)

رقم	العبرة
5.	أدت تقنيات التحول الرقمي إلى ظهور مخاطر سيبرانية جديدة تتطلب إجراءات رقابية مختلفة.
6.	يتم تكيف وتحديث الضوابط الداخلية باستمرار لتواكب سرعة التغيرات في الأنظمة والمنتجات الرقمية الجديدة.
7.	ساهمت أنظمة المراقبة الآلية التي يوفرها التحول الرقمي في الكشف المبكر عن المخاطر التشغيلية وتقليل زمن الاستجابة لها.
8.	يمتلك البنك إطاراً قوياً لإدارة مخاطر الطرف الثالث (Third-Party Risk) الناتجة عن التعامل مع شركات التكنولوجيا المالية (FinTech).

الفصل الرابع

النتائج الإحصائية والتحليل الوصفي (عينة 100)

تم إجراء التحليل الإحصائي على بيانات 100 استبيان مكتمل من العاملين في البنوك السعودية.

أولاً: تحليل البيانات الديموغرافية للعينة (ن=100)

المتغير	الفئة	التكرار (Frequency)	النسبة المئوية (%)
المسمى الوظيفي	مدير قسم / رئيس وحدة	35	35.0%
	موظف متخصص / محلل	50	50.0%
	مدير تنفيذي (C- Level/General (Management	15	15.0%

سنوات الخبرة	أقل من 5 سنوات	20	%20.0
	5 - 10 سنوات	45	%45.0
	10 سنوات فأكثر	35	%35.0
الإدارة	إدارة المخاطر	40	%40.0
	العمليات المصرفية	30	%30.0
	تقنية المعلومات/التحول الرقمي	30	%30.0

ثانياً: تحليل المحور المستقل: التحول الرقمي (ن=100)

الهدف: قياس مستوى تبني التقنيات الرقمية المتقدمة في العمليات المصرفية.

العبارة	المتوسط الحسابي (Mean)	الانحراف المعياري (SD)	مستوى التبني (التقدير)
---------	------------------------------	------------------------------	------------------------------

مرتفع	0.85	4.15	1. يعتمد البنك على أنظمة الذكاء الاصطناعي (AI) في أتمتة الإجراءات التشغيلية الأساسية.
مرتفع	1.02	3.92	2. تُستخدم تحليلات البيانات الضخمة (Big Data Analytics) للتنبؤ بالخسائر التشغيلية المحتملة.
متوسط	1.15	3.10	3. تم نقل معظم الأنظمة المصرفية الأساسية في البنك إلى بيئة الحوسبة السحابية.
مرتفع جداً	0.70	4.45	4. يساهم التبني الرقمي في تقليل الاعتماد على التدخل البشري وبالتالي يحد من الأخطاء التشغيلية اليدوية.

المتوسط العام للمحور	3.91	0.93	مرتفع
----------------------	------	------	-------

التحليل الأولي للمحور:

يشير المتوسط العام المرتفع (3.91) إلى أن البنوك السعودية تتبنى التحول الرقمي بمستوى مرتفع. وتظهر العبارة (4) أعلى متوسط (4.45)، مما يؤكد الإجماع على أن التحول الرقمي هو أداة فعالة للحد من الأخطاء التشغيلية الناتجة عن العنصر البشري.

ثالثاً: تحليل المحور التابع: فاعلية إدارة المخاطر التشغيلية (ن=100)

الهدف: قياس كفاءة إدارة المخاطر في البيئة الرقمية.

العبارة	المتوسط الحسابي (Mean)	الانحراف المعياري (SD)	مستوى الفاعلية (التقدير)
5. أدت تقنيات التحول الرقمي إلى ظهور مخاطر سيبرانية جديدة تتطلب إجراءات رقابية مختلفة.	4.60	0.65	مرتفع جداً

مرتفع	0.90	3.88	6. يتم تكييف وتحديث الضوابط الداخلية باستمرار لتواكب سرعة التغيرات في الأنظمة والمنتجات الرقمية الجديدة.
مرتفع	0.75	4.25	7. ساهمت أنظمة المراقبة الآلية التي يوفرها التحول الرقمي في الكشف المبكر عن المخاطر التشغيلية وتقليل زمن الاستجابة لها.
متوسط/مرتفع	1.05	3.65	8. يمتلك البنك إطاراً قوياً لإدارة مخاطر الطرف الثالث (FinTech).
مرتفع	0.84	4.09	المتوسط العام للمحور

التحليل الأولي للمحور:

بلغ المتوسط العام لهذا المحور 4.09 (مرتفع)، مما يشير إلى أن العاملين يرون فاعلية عالية نسبياً لإدارة المخاطر في البيئة الرقمية. وتبرز العبارة (5) أعلى متوسط (4.60)، مما يمثل إجماعاً قوياً على أن ظهور المخاطر السيبرانية هو الأثر الأكبر للتحول الرقمي، وهو ما يجب التركيز عليه في نتائج التحليل.

رابعاً: نتائج اختبار الفرضية الرئيسية (تحليل الانحدار)

الفرضية: يوجد أثر ذو دلالة إحصائية للتحويل الرقمي على فاعلية وكفاءة إدارة المخاطر التشغيلية في العمليات المصرفية بالبنوك السعودية.

المؤشر	القيمة	الدلالة الإحصائية	النتيجة
معامل الارتباط (\$R\$)	0.758	0.000	علاقة قوية وموجبة
معامل التحديد (\$R^2\$)	0.574	–	يفسر المتغير المستقل 57.4% من التباين في المتغير التابع

قيمة (\$F\$)	131.95	0.000	دال إحصائياً عند مستوى 0.01
معامل الانحدار (\$\beta\$) للتحويل الرقمي	0.685	0.000	يوجد أثر مباشر وإيجابي قوي

النتيجة النهائية:

بناءً على النتائج، تم رفض فرضية العدم وقبول الفرضية الرئيسية (H1). يوجد أثر إيجابي وقوي ذو دلالة إحصائية للتحويل الرقمي على فاعلية وكفاءة إدارة المخاطر التشغيلية في البنوك السعودية. ويشير معامل الانحدار إلى أن زيادة مستوى التحويل الرقمي بوحدة واحدة يؤدي إلى زيادة فاعلية إدارة المخاطر بحوالي 0.685.

نتائج الدراسة (Findings)

بناءً على التحليل الإحصائي للبيانات المجمعة من عينة الدراسة البالغة 100 فرد من العاملين في البنوك السعودية، خلصت الدراسة إلى النتائج الرئيسية التالية:

1. النتائج المتعلقة بالفرضية الرئيسية

نتيجة الفرضية الرئيسية: تم قبول الفرضية التي تنص على "وجود أثر إيجابي وقوي ذي دلالة إحصائية للتحويل الرقمي على فاعلية وكفاءة إدارة المخاطر التشغيلية في العمليات المصرفية بالبنوك السعودية".

• **قوة العلاقة:** أظهر معامل الارتباط ($R=0.758$) وجود علاقة طردية قوية جداً

بين متغير التحويل الرقمي وفاعلية إدارة المخاطر التشغيلية.

• **الأثر التفسيري:** أشار معامل التحديد ($R^2=0.574$) إلى أن التحويل الرقمي

يفسر أكثر من نصف التباين (57.4%) في فاعلية إدارة المخاطر التشغيلية، مما

يؤكد أهميته كعامل محوري.

2. النتائج المتعلقة بالمتغير المستقل (التحويل الرقمي)

• **التبني الرقمي مرتفع:** أظهر المتوسط العام لمحور التحويل الرقمي (3.91) أن

البنوك السعودية لديها مستوى تبني مرتفع للتقنيات الرقمية المتقدمة في عملياتها.

• **الكفاءة التشغيلية:** هناك إجماع (بمتوسط 4.45) على أن التبني الرقمي يساهم

بشكل فعال ومباشر في تقليل الأخطاء التشغيلية اليدوية الناتجة عن التدخل

البشري.

• استخدام الذكاء الاصطناعي: يُستخدم الذكاء الاصطناعي والتعلم الآلي بشكل

كبير (متوسط 4.15) في أتمتة الإجراءات التشغيلية، مما يعزز سرعة ودقة

العمليات.

3. النتائج المتعلقة بالمتغير التابع (فاعلية إدارة المخاطر التشغيلية)

• ظهور مخاطر جديدة (الأثر السلبي): أكدت العينة بأغلبية ساحقة (بمتوسط

4.60) أن أبرز أثر للتحويل الرقمي هو ظهور مخاطر سيبرانية جديدة ومعقدة

تتطلب ضوابط رقابية متخصصة ومختلفة عن الضوابط التقليدية.

• دور المراقبة الآلية: ساهمت أنظمة المراقبة الآلية المدعومة بالذكاء الاصطناعي

بشكل كبير (متوسط 4.25) في تحسين الكشف المبكر عن المخاطر التشغيلية

وتقليص زمن الاستجابة للحوادث.

• مخاطر الطرف الثالث: لوحظ أن إدارة مخاطر الطرف الثالث (مثل التعامل مع

شركات التكنولوجيا المالية FinTech) تتمتع بفاعلية متوسطة إلى مرتفعة (متوسط

3.65)، مما يشير إلى الحاجة لمزيد من التعزيز في هذا الجانب.

• مواءمة الضوابط: أظهرت النتائج أن هناك جهوداً جادة لتكييف وتحديث الضوابط

الداخلية لتواكب التغيرات الرقمية السريعة (متوسط 3.88).

خلاصة النتائج: التحول الرقمي هو عامل تمكين قوي لفاعلية إدارة المخاطر التشغيلية، لكنه يأتي مصحوباً بضرورة التعامل الفوري والمكثف مع المخاطر المستحدثة، وفي مقدمتها الأمن السيبراني.

توصيات الدراسة (Recommendations)

بناءً على النتائج التي توصلت إليها الدراسة، تُقدم التوصيات التالية للجهات المعنية في القطاع المصرفي السعودي (البنوك والجهات الرقابية):

1. التوصيات المتعلقة بالتحول الرقمي وإدارة المخاطر (التكامل)

• **تطبيق منظور "المخاطر في التصميم" (Risk by Design):** يجب على البنوك

دمج اعتبارات ومتطلبات إدارة المخاطر التشغيلية والأمن السيبراني في المراحل الأولية لتصميم أي منتج أو نظام رقمي جديد، بدلاً من إضافتها لاحقاً كعلاج.

• **تطوير نماذج المخاطر التنبؤية:** ضرورة الاستثمار في تقنيات التعلم الآلي

(Machine Learning) لتدريب النماذج على كميات كبيرة من البيانات

التشغيلية لتوقع الخسائر المحتملة قبل وقوعها، بدلاً من الاعتماد على البيانات التاريخية فقط.

• **تعزيز حوكمة البيانات:** إنشاء إطار حوكمة شامل للبيانات يضمن جودة،

وخصوصية، وأمن البيانات المستخدمة في الأنظمة الرقمية، لأن جودة المخرجات

الرقابية تعتمد مباشرة على جودة البيانات المدخلة.

2. التوصيات المتعلقة بمعالجة المخاطر المستحدثة (الأمن السيبراني والطرف الثالث)

- رفع مستوى الأمن السيبراني كأولوية قصوى: تخصيص ميزانيات أعلى لتعزيز

البنية التحتية للأمن السيبراني، مع التركيز على أنظمة الكشف والاستجابة المتقدمة

(XDR) واختبار الاختراق المنتظم (Penetration Testing) للقنوات الرقمية.

- إدارة مخاطر الطرف الثالث (FinTech): وضع معايير صارمة وموحدة لتقييم

المخاطر التشغيلية المرتبطة بالتعاقد مع شركات التكنولوجيا المالية (FinTech)

ومقدمي الخدمات السحابية، والتأكد من توافق ضوابطهم مع متطلبات البنك

المركزي السعودي (SAMA).

3. التوصيات المتعلقة بالتدريب والتطوير

- برامج تدريب متخصصة: تصميم برامج تدريبية متقدمة ومتعددة التخصصات

(Cross-functional) تجمع بين موظفي إدارة المخاطر وموظفي تقنية

المعلومات، لتمكينهم من فهم المخاطر التشغيلية من منظور تكنولوجي.

- تطوير الكفاءات في التحليل الكمي: الاستثمار في بناء قدرات داخلية على تحليل

البيانات الضخمة والنماذج الإحصائية المتقدمة لقياس المخاطر التشغيلية، بعيداً

عن الطرق التقليدية.

4. التوصيات للجهات الرقابية (البنك المركزي السعودي SAMA)

- **تحديث الأطر الرقابية:** تحديث الإطار الرقابي لإدارة المخاطر التشغيلية بشكل دوري ومستمر ليوافق التقنيات الناشئة مثل الذكاء الاصطناعي التوليدي، وضمان وجود ضوابط خاصة لهذه التقنيات.
- **تشجيع تبادل الخبرات:** إنشاء منصات لتبادل الخبرات بين البنوك حول أفضل الممارسات في التعامل مع الحوادث السيبرانية الأخيرة والخسائر التشغيلية الناتجة عن فشل الأنظمة الرقمية.

قائمة المراجع (References)

أولاً: المراجع العربية

1. أبو غبن، أ.، و المدهون، م. (2018). دور التحول الرقمي في تحقيق التميز المؤسسي بالتطبيق على العاملين في بلدية غزة. مجلة الجامعة الإسلامية للدراسات الاقتصادية والإدارية.
2. إسماعيل، ع. ر. (2021). دور انترنت الأشياء في إدارة معرفة العملاء بالتطبيق على البنوك التجارية العامة في مصر. المجلة العلمية للدراسات التجارية والبيئية.
3. بارة، ز. (2020). إدارة المخاطر المصرفية وفق مقررات بازل 3 [رسالة ماجستير غير منشورة]. جامعة باجي مختار، الجزائر.
4. البشير، ف. ع. (2010). المخاطر التي تواجه المصارف الإسلامية وآليات مقترحة للحد منها. مركز أبحاث الاقتصاد الإسلامي.
5. البناء، أ.، و جاد الله، ب.، و العجمي، ع. (2024). متطلبات تفعيل الرقمنة في الجامعات الحكومية الكويتية على ضوء خبرات بعض الدول المتقدمة. المجلة العلمية لكلية التربية - جامعة أسيوط.

6. بوعلي، د. (2015). إدارة المخاطر المصرفية بين البنوك التقليدية والبنوك الإسلامية [رسالة ماجستير غير منشورة]. جامعة المسيلة، الجزائر.
7. بوشدوب، ط.، و زورداني، ش. (2021). دور البلوكشين في التقليل من مخاطر التمويل الإسلامي. مجلة الاقتصاد والإحصاء التطبيقي.
8. الحريث، م.، و حزوري، ح. (2018). مخاطر الائتمان وأثرها في كفاية رأس المال المصرفي. مجلة جامعة القدس المفتوحة.
9. حياصات، م. (2022). دور الحوسبة السحابية في تطوير أداء العاملين - البنوك التجارية الأردنية [رسالة ماجستير غير منشورة]. جامعة البلقاء، الأردن.
10. الخفاجي، ه. (2017). تفعيل إدارة المخاطر المصرفية في ظل تكنولوجيا المعلومات والاتصالات [رسالة ماجستير غير منشورة]. الأكاديمية العربية للعلوم المالية والمصرفية، الأردن.
11. د. مارية عواوده (2025). إدارة المخاطر المصرفية في ظل التحول الرقمي. مجلة رماح للبحوث والدراسات، 116(2).
12. رجب، إ. (2022). التحول الرقمي في التعليم الجامعي [رسالة ماجستير غير منشورة]. جامعة جنوب الوادي، مصر.

13. رضوان، ط. ذ. (2024). تطبيق الذكاء الاصطناعي على ممارسات إدارة

الموارد البشرية دراسة تطبيقية على العاملين بمصلحة الضرائب المصرية [رسالة

ماجستير غير منشورة]. جامعة طنطا، مصر.

14. زهر، إ. م.، و حامد، أ. ع. (2024). أثر التحول الرقمي على إدارة

المخاطر المصرفية -دراسة حالة. المجلة العلمية للبحوث التجارية.

15. صلاح الدين، ث. (2023). أثر التحول الرقمي على أداء مؤسسات التعليم

العالي [رسالة ماجستير غير منشورة]. جامعة الجليلي بونعامة، الجزائر.

16. عاشور، م. (2020). الشبكات العصبية الاصطناعية. جامعة بغداد.

17. العبد الله، ن. (2021). دور حوكمة تكنولوجيا المعلومات في الحد من

المخاطر المصرفية الإلكترونية: دراسة ميدانية. مجلة الدراسات والبحوث التجارية

- جامعة بنها.

18. علاوي، ع. م. (2012). إدارة مخاطر التشغيل في المصارف الإسلامية

دراسة مقارنة بين المصارف الإسلامية في السودان والأردن [رسالة ماجستير غير

منشورة]. جامعة أم درمان، السودان.

19. فيها خير، ج. (2012). إدارة المخاطر الائتمانية في البنوك الإسلامية

دراسة حالة بنك البركة الجزائري [رسالة ماجستير غير منشورة]. جامعة قاصدي

مرباح، الجزائر.

20. المطيري، أ. (2018). الحوسبة السحابية المفهوم والتطبيقات. مجلة كلية

الآداب، جامعة سوهاج.

21. ناولو، م. (2022). إدارة المخاطر المالية والمصرفية بين النظرية

والتطبيق. دار سورية الفتاة.

22. النجداوي، ب. (2019). مخاطر السيولة في البنوك الإسلامية [رسالة

ماجستير غير منشورة]. جامعة البلقاء، الأردن.

23. الهلالي، م. (2021). التحول الرقمي في عصر البيانات الضخمة. المجلة

العربية الدولية للتكنولوجيا المعلومات.

ثانياً: المراجع الأجنبية (English References)

1. **Aziz, S & ,Dowling, M .(2019) .Machine Learning and AI**

for Risk Management .Palgrave Studies in Digital Business

and Enabling Technologies.

2. **Czapran, T .(2023) .IMPLEMENTATION OF MICROSOFT**

DYNAMICS 365 .The International Scientific Conference

Economic Policy.

3. **Gunduz, V .(2020) .Management & Strategy Risk**

Management in Banking Sector .Artikel Akademi.

4. **Rosati, P & ,.Čuk, T** .(2019) .Blockchain Beyond Cryptocurrencies .Palgrave Studies in Digital Business and Enabling Technologies.
5. **Salama, A** .(2021) .Risk Management Techniques on the Internet of Things .Journal of Computer Science and Information Systems, 2.3 ,(5)
6. **Schwertner, K** .(2017) .DIGITAL TRANSFORMATION OF BUSINESS .Trakia Journal of Sciences, 15.
7. **Senyo, P. K., Effah, J & ,.Addae, E** .(2016) .Preliminary insight into cloud computing adoption in a developing country .Journal of Enterprise Information Management, 29.(4)
8. **Shendge, A** .(2021) .INTERNET OF THINGS (IOT): AN OVERVIEW ON RESEARCH CHALLENGES AND FUTURE APPLICATIONS .International Journal of Engineering Applied Sciences and Technology, 6.(8)

9. **Tursoy, T** .(2018) .Risk management process in banking industry .Munich Personal RePEc Archive) .Paper No. 86427.(

10. **Yahaya, A** .(2024) .The impact of risk management committee on firm risk, with risk management practices as a mediator .Journal of Applied Corporate Finance, 11.(113)

ملخص الدراسة (Abstract)

هدفت هذه الدراسة إلى تقييم الأثر الصافي للتحويل الرقمي على فاعلية وكفاءة إدارة المخاطر التشغيلية في العمليات المصرفية بالبنوك السعودية. اعتمدت الدراسة على المنهج الوصفي التحليلي، وتمثلت أداة جمع البيانات في استبيان وُزِعَ على عينة قصدية من (100) مختص في إدارات المخاطر والعمليات وتقنية المعلومات بالبنوك السعودية. أظهرت النتائج الإحصائية الرئيسية ما يلي:

5. قبول الفرضية الرئيسية: أثبتت الدراسة وجود أثر إيجابي وقوي ذي دلالة إحصائية للتحويل الرقمي على فاعلية إدارة المخاطر التشغيلية (معامل ارتباط $R=0.758$)، حيث يساهم التحويل الرقمي في تحسين كفاءة آليات الرقابة والكشف عن المخاطر.

6. التحدي الأبرز: أكد المشاركون أن ظهور وتفاقم المخاطر السيبرانية هو الأثر السلبي الأبرز المصاحب للرقمنة، مما يفرض ضغوطاً متزايدة على أطر إدارة المخاطر.

7. مكسب الكفاءة: يوجد إجماع على أن التحويل الرقمي ينجح في تقليل الأخطاء التشغيلية اليدوية الناتجة عن العنصر البشري بشكل كبير، مما يعزز الاستقرار التشغيلي.

8. دور التقنيات: ساهمت أنظمة المراقبة الآلية المعتمدة على الذكاء الاصطناعي في

تحسين الكشف المبكر عن المخاطر وتقليص زمن الاستجابة للحوادث.

بناءً على النتائج، أوصت الدراسة البنوك بضرورة تبني مبدأ "المخاطر في التصميم"

(Risk by Design) في تطوير المنتجات الرقمية، ورفع مستوى الاستثمار في الأمن

السيبراني، وتطوير برامج تدريب متخصصة تجمع بين الجوانب التكنولوجية والرقابية

لمواجهة التحديات الجديدة في العصر الرقمي.

الملاحق

هيكل وأسئلة الاستبيان

الهدف العام للاستبيان

الهدف من هذا الاستبيان هو جمع بيانات أولية لتقييم مدى تبني البنوك السعودية لأدوات

التحول الرقمي وتحديد الأثر الناتج عن هذا التبني على فاعلية وكفاءة إدارة المخاطر

التشغيلية لديها.

مقياس الإجابة

سيتم استخدام مقياس ليكرت الخماسي لجميع عبارات محاور الدراسة، حيث تكون

الخيارات هي:

1 = أوافق بشدة (Strongly Agree)

2 = أوافق (Agree)

3 = محايد (Neutral)

4 = لا أوافق (Disagree)

5 = لا أوافق بشدة (Strongly Disagree)

أولاً: البيانات الديموغرافية (التعريفية)

(تُصاغ كخيارات متعددة بسيطة أو إجابة مفتوحة قصيرة)

1. المسمى الوظيفي: (مدير إدارة، رئيس قسم، موظف متخصص، إلخ)

2. سنوات الخبرة الإجمالية في القطاع المصرفي: (أقل من 5 سنوات، 5-10

سنوات، 10 سنوات فأكثر)

3. الإدارة التي تنتمي إليها: (إدارة المخاطر، العمليات المصرفية، تقنية

المعلومات/التحول الرقمي، التدقيق والامتثال)

4. المستوى التعليمي: (بكالوريوس، ماجستير، دكتوراه)

ثانياً: محور قياس المتغير المستقل: التحول الرقمي (4 عبارات)

(يهدف إلى قياس مستوى تبني التقنيات الرقمية المتقدمة في العمليات المصرفية)

رقم	العبرة
1.	يعتمد البنك على أنظمة الذكاء الاصطناعي (AI) في أتمتة الإجراءات التشغيلية الأساسية (مثل مطابقة المستندات).
2.	تُستخدم تحليلات البيانات الضخمة (Big Data Analytics) بشكل فعال للتنبؤ بالخسائر التشغيلية المحتملة.
3.	تم نقل معظم الأنظمة المصرفية الأساسية في البنك إلى بيئة الحوسبة السحابية (Cloud Computing).
4.	يساهم التبني الرقمي في تقليل الاعتماد على التدخل البشري وبالتالي يحد من الأخطاء التشغيلية اليدوية.

ثالثاً: محور قياس المتغير التابع: فاعلية إدارة المخاطر التشغيلية (4 عبارات)

(يهدف إلى قياس كفاءة إدارة المخاطر في البيئة الرقمية)

رقم	العبارة
5.	أدت تقنيات التحول الرقمي إلى ظهور مخاطر سيبرانية جديدة تتطلب إجراءات رقابية مختلفة.
6.	يتم تكيف وتحديث الضوابط الداخلية باستمرار لتواكب سرعة التغيرات في الأنظمة والمنتجات الرقمية الجديدة.
7.	ساهمت أنظمة المراقبة الآلية التي يوفرها التحول الرقمي في الكشف المبكر عن المخاطر التشغيلية وتقليل زمن الاستجابة لها.
8.	يملك البنك إطاراً قوياً لإدارة مخاطر الطرف الثالث (Third-Party Risk) الناتجة عن التعامل مع شركات التكنولوجيا المالية (FinTech).

MidOcean University

College of Management

Department/Specialization:

Master of Science in Risk Management



Research Title

**The Impact of Digital Transformation on Operational Risk
Management in Banks: A Field Study on Banking Operations
in Saudi Banks**

Prepared by:

Ayman Hussein Bareidah

Supervision:

Dr. Al-Faisal Abdulhamid Mohammed

Dafayez Ali Al-Jarrad

Academic Year:

2025