

بحث عن

فاعلية تقنية المعلومات في الوقاية من الاحتيال بالبنوك التجارية السعودية

إعداد الطالبة

رنا عطالله الفائدي

إشراف

د/ الفیصل عبد الحمید حسن

د/ وليد سليمان

العام الدراسي

1445هـ/2024م

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

قُلْ أَتَدْعُونِي إِلَى عِلْمٍ

صَدَقَ اللَّهُ الْعَظِيمَ

سُرَّةُ الْقَلْبِ

الحمد لله رب العالمين والصلاة والسلام على أشرف المرسلين المبعوث رحمة للعالمين نبينا محمد النبي الأمي وعلى آله وصحبه وسلم.

بداية أتقدم بالشكر وعظيم الامتنان لكل الأساتذة والدكاترة بكلية الإدارة جامعة الجميع الذكية، وذلك لما بذلوه مخلصين في مسؤولياتهم العلمية تجاه طلبه الكلية، والذين قدموا لي ولزملائي خاصة خبراتهم ومعارفهم وأخص بالشكر والعرفان كلا من:

الأستاذ الدكتور/ وليد سليمان

والأستاذ الدكتور/ الفيصل عبد الحميد حسن

اللذان تواضعا مشكورين وأشرفا على هذه الدراسة ولم يدخرأ جهداً معي في توفير المعلومة والملاحظة من أجل إنجاز هذه الدراسة.

وأقدم بالشكر والعرفان لإدارة الكلية وعلى رأسهم سعادة العميد وسعادة رئيس القسم.

وأشكر كل الذين تعاونوا بشكل أو بآخر معي لإنجاز واتمام هذه الدراسة.

الباحثة

قائمة المحتويات

الصفحة	الموضوع
2	الجزء الأول: (التمهيد) آية قرآنية.
3	شكر وتقدير.
4	قائمة المحتويات.
5	قائمة الجداول والأشكال.
5	قائمة الملاحق.
6	المقدمة:
7	أهمية الدراسة.
7	منهج الدراسة.
7	إشكالية الدراسة.
8	أهداف الدراسة.
8	أسئلة الدراسة.
9	الجزء الثاني: الإطار النظري للدراسة
9	المبحث الأول: تقنية المعلومات.
10	المطلب الأول: أهمية تقنية المعلومات.
11	المطلب الثاني: آلية عمل تقنية المعلومات من الوقاية من الاحتيال لدى البنوك التجارية.
12	المطلب الثالث: دور تقنية المعلومات في مكافحة عمليات الاحتيال.
15	المبحث الثاني: الاحتيال.
15	المطلب الأول: تعريف الاحتيال.
18	المطلب الثاني: دور التقنية.
19	المطلب الثالث: خطة مكافحة الاحتيال.
23	المطلب الرابع: لجنة مراقبة الاحتيال.
25	المطلب الخامس: تحليل الاحتيال.
26	الدراسات السابقة
26	الدراسات العربية
26	الدراسات الأجنبية
28	الجزء الثالث: الدراسة العملية والإجراءات المنهجية

28	المنهجية وطرق البحث
28	مجتمع الدراسة والعينة.
28	متغيرات الدراسة.
28	أسلوب وأداة جمع البيانات.
29	الطرق الإحصائية المستخدمة.
29	أساليب المعالجة الإحصائية.
30	أولاً: الإحصاءات الوصفية للمتغيرات الشخصية.
31	ثانياً: صدق وثبات أداة جمع البيانات.
32	طرق حساب الثبات.
35	ثالثاً: الإحصاءات الوصفية للعبارات على شكل مقياس ليكرت (المعدل).
37	الجزء الرابع: ملاحق الدراسة.
40	نتائج الدراسة.
41	التوصيات
42	قائمة المراجع والمصادر.
44	الملاحق.

قائمة الجداول والأشكال

الصفحة	المحتوى	مسلسل
14	دور تقنية المعلومات في مكافحة عملية الاحتيال.	شكل رقم (1)

قائمة الملاحق

الرقم	الملاحق	الصفحة
1	الاستبيان	44

المقدمة:

تعتبر التكنولوجيا المعلوماتية أداة حيوية في الوقاية من الاحتيال في البنوك التجارية. تعمل هذه التقنيات على تعزيز أمان المعاملات المالية وحماية العملاء والبنوك من الاحتيال المحتمل، تهدف هذه الدراسة إلى دراسة فعالية تقنية المعلومات في الوقاية من الاحتيال في البنوك التجارية، وتحليل أفضل الممارسات والتقنيات المستخدمة في هذا السياق، بالإضافة إلى تقديم توصيات لتحسين استخدام التكنولوجيا لمكافحة الاحتيال في البنوك.

إن استخدام تقنية المعلومات في الوقاية من الاحتيال من أفضل من النظم الرقابية لحماية موارد المجتمع بأكمله، كما أن استخدام تقنية المعلومات في الوقاية من الاحتيال في البنوك التجارية يؤدي إلى الحصول على المعلومات في الوقت المناسب، ومع استخدام تقنية المعلومات في الوقاية من الاحتيال تنتج معلومات تتصف بالمصداقية وامكانية الاعتماد عليها لاتخاذ قرارات إدارية رشيدة لصالح الهيئة أو المؤسسة.

ويعتبر مفهوم تقنية المعلومات من المفاهيم الحديثة نسبياً، فهو يرتبط بمهمة جمع البيانات، ومعالجتها، وتخزينها، وتحديثها، واسترجاعها، حيث تعرف التقنية هنا بأنها تطبيق الإجراءات المستمدة من البحث العلمي والخبرات العلمية لحل المشكلات الواقعية، وتعني التقنية الأسس النظرية والعلمية والأدوات والمكائن التي ترمي إلى تحسين الأداء البشري في الحركة التي تتناولها.

لذا أصبح من الضرورة استخدام تقنية المعلومات في الوقاية من الاحتيال في البنوك التجارية السعودية لحماية مواردها، مع تطوير الإجراءات الوقائية، لأن استخدام تقنية المعلومات انتشر في العديد من المجالات، مع ما تحققه تلك التقنية من سرعة ودقة في الأداء، خاصة مع تطور وتعقد مختلف العمليات الإدارية والتشغيلية وصعوبة مراقبتها، ومن هنا أصبح الاعتماد عليها لتسهيل وتسريع عمليات الرقابة.

إن الفرص التي تخلقها تقنيات المعلومات تمثل تحدياً خاصاً للمؤسسات المصرفية، مع استمرارها في الابتكار في إيجاد وتقديم طرق جديدة للوصول إلى العملاء، فإن تلك المؤسسات تتعرض في الوقت نفسه لمخاطر جديدة. حيث إن الاستخدام الضار لتقنية المعلومات يمكن أن يؤدي إلى تعطيل الخدمات المالية الضرورية للأنظمة المالية الوطنية والدولية، وتقويض الأمن والثقة، وتعريض الاستقرار المالي للخطر. إن طرق الاحتيال الالكترونية تشكل تهديداً للنظام المالي بأكمله، وهي حقيقة تؤكدتها التقارير الصادرة في هذا الشأن على المستوى الدولي والإقليمي والمحلي، وفي هذا السياق تشير تقارير البنك الدولي إلى تركيز الهجمات السيبرانية في قطاع الخدمات المالية الذي

شهد في عام 2016م هجمات سيبرانية تفوق القطاعات الأخرى بنسبة 65%.

أهمية الدراسة:

يجب أن نؤكد على أهمية استخدام تقنية المعلومات في الوقاية من الاحتيال في البنوك التجارية العاملة في المملكة العربية السعودية من خلال:

- حماية العملاء حيث تساهم الدراسة في تحسين الأمان المالي للعملاء من خلال تحسين التقنيات المستخدمة في مكافحة الاحتيال، مما يزيد من ثقتهم في البنوك ويحيي أموالهم.
- حماية المؤسسات المالية حيث تعزز الدراسة قدرة البنوك التجارية على الدفاع عن أنفسها ضد مختلف أشكال الاحتيال، مما يحيي سمعتها ويقلل من خسائرها المالية والسلبية.
- دعم التطور التكنولوجي حيث تساهم الدراسة في دفع عجلة التطور التكنولوجي في قطاع البنوك التجارية داخل المملكة من خلال تحليل وتقييم الأدوات والتقنيات الحديثة المستخدمة في مكافحة الاحتيال وتوجيه الاستثمارات نحو الحلول الأكثر فعالية.
- تحسين القرارات الإدارية حيث توفر الدراسة أدلة قوية وتحليلاً دقيقاً يمكن استخدامها من قبل الإدارات في البنوك لاتخاذ قرارات استراتيجية بشأن استثمارات تقنية المعلومات لمكافحة الاحتيال.
- تعزيز الأمن الاقتصادي من خلال مكافحة الاحتيال في البنوك، يمكن تعزيز الاستقرار الاقتصادي عن طريق منع خسائر مالية كبيرة للفرد والمؤسسة، وبالتالي تحقيق بيئة مالية أكثر أماناً واستقراراً.

منهج الدراسة:

من أجل الإجابة على الإشكالية السابقة، تم الاعتماد على المنهج الوصفي التحليلي للإحاطة بالجوانب المتعلقة بفاعلية تقنية المعلومات في الوقاية من الاحتيال بالبنوك التجارية السعودية، كما تم الاعتماد أيضاً على أسلوب دراسة الحالة للتعرف على واقع تقنية المعلومات في البنوك التجارية.

إشكالية الدراسة:

تتمثل مشكلة الدراسة في:

1. مدى فاعلية تقنية المعلومات في الوقاية من الاحتيال في البنوك التجارية السعودية.
2. مدى استخدام تقنية المعلومات لزيادة فاعلية الوقاية من الاحتيال في البنوك التجارية السعودية.

3. مدة استخدام تقنية المعلومات في الوقاية من الاحتيال في البنوك التجارية السعودية وما ينتج عنها من

معلومات تتصف بالمصادقية.

أهداف الدراسة:

1. تحليل أنواع الاحتيال الشائعة في البنوك التجارية.
2. فهم كيفية توظيف تقنية المعلومات في الوقاية من الاحتيال في البنوك.
3. دراسة الأدوات والتقنيات المستخدمة في الكشف عن الاحتيال والوقاية منه.
4. تقييم فعالية استخدام تقنية المعلومات في الحد من الاحتيال في البنوك التجارية.
5. تقديم توصيات لتحسين استخدام تقنية المعلومات في مكافحة الاحتيال في البنوك.

أسئلة الدراسة:

تتمثل أسئلة الدراسة في:

- ما هي أهم التقنيات المستخدمة في مكافحة الاحتيال في البنوك التجارية السعودية؟
- كيف يمكن تصنيف أنواع الاحتيال المتعددة التي تستهدف البنوك؟
- ما هي التحديات التقنية التي تواجه استخدام تقنية المعلومات في الوقاية من الاحتيال؟
- ما هي أفضل الممارسات والتقنيات الحالية المستخدمة في الكشف عن الاحتيال والوقاية منه في البنوك التجارية السعودية؟

الجزء الثاني

الإطار النظري للدراسة

إن استخدام تقنية المعلومات أصبح ضرورة حتمية نظراً للمزايا الكبيرة التي تتمتع بها، ولهذا تسابقت الدول من أجل استغلالها واستخدامها، للانتقال من الإدارة التقليدية إلى الإدارة الإلكترونية، ومواكبة التطورات العالمية المتسارعة، حيث تلعب الشبكة العنكبوتية أو الإنترنت دوراً وتأثيراً كبيراً في تكوين الرأي العام وتشكيله، وقد أظهرت النتائج أن نسبة من تعرضوا لخطاب الكراهية عبر وسائل الإعلام الجديد هي النسبة الأكبر والتي تدل على أن هناك تربة خصبة وممارسة فعلية لخطاب الكراهية عبر (الشبكة العنكبوتية) ولم تكن الدول العربية بمنأى عن مواكبة التطورات المتلاحقة في هذا المجال، وحاولت بعضها التطور وبدرجات متفاوتة، فبعض الدول تبنت استراتيجية واضحة في سبيل ذلك، لكن بقية الدول ما زالت تواجه تحديات جمة في سبيل الحد من الهوة بينها وبين غيرها من الدول المتقدمة، نظراً لعدة عوامل تتوزع بين الفقر والجهل، ولكن باستطاعة هذه الدول تحسين مراتبها في هذا المجال، إذا توفرت متطلبات تطبيق الإدارة الإلكترونية، لأن معيار التقدم الآن حسب تقارير الأمم المتحدة هو مدى قدرة الدول على مواكبة الثورة المعلوماتية وحتمية تطبيقها، ولإزال أمام الدول العربية الكثير من الجهود لبذلها حتى تتمكن من مواكبة التطورات المتلاحقة في هذا المجال.

وفي ظل التطورات التقنية التي جاءت بفعل ظاهرة العولمة، سعت المنظمات والهيئات العاملة في مجال تقنية المعلومات إلى تحديث نظمها، من خلال استخدام الوسائل الإلكترونية المستحدثة، مما استوجب وضع نظام معلوماتي يحمي الفرد والهيئة على حد سواء من الاعتداءات والاختراقات.

المبحث الأول: تقنية المعلومات:

أثبتت تقنية المعلومات بأدواتها وآلياتها أهميتها البالغة، فلم يؤثر شيء في الحياة الإنسانية منذ الثورة الصناعية مثلما أثرت فيها تكنولوجيا المعلومات وما أحدثته من تغيرات في المعاملات والتواصل، والتي أصبحت لا غنى عنها في حياة الشعوب والمؤسسات والدول، فما يشهده العالم من تحول تقني متسارع، بجانب التطورات المتلاحقة في مجال أجهزة الحاسوب والبرمجيات وأجهزة الاتصالات ووسائلها، وهذا الكم الهائل من المعلومات الذي ينمو وينتقل بسهولة ويسر.

إنّ تقنية المعلومات أو تكنولوجيا المعلومات IT هي عبارة عن أيّ تقنية تعمل على تحقيق إمكانية تخزين ومعالجة وتدفع المعلومات داخل مؤسسة ما، مع كل ما يتعلق بأجهزة الكمبيوتر والبرامج والشبكات الداخلية، مواقع الويب، الخوادم، قواعد البيانات وكذلك الاتصالات السلكية واللاسلكية..... كل ذلك يقع تحت مظلة تقنية المعلومات.

تقنية المعلومات تشير إلى استخدام الحواسيب والبرمجيات والشبكات والأنظمة الإلكترونية لجمع وتخزين ومعالجة ونقل المعلومات. وتشمل تقنية المعلومات جميع الأدوات والتقنيات التي تساعد في إدارة وتحليل وتبادل المعلومات بشكل فعال وفي الوقت المناسب.

تقنية المعلومات تلعب دورًا حيويًا في تحسين الأعمال وتعزيز الإنتاجية في مختلف القطاعات، بما في ذلك القطاع المالي، وتشمل تطبيقات تقنية المعلومات في البنوك التجارية تحسين خدمات العملاء، وتبسيط العمليات الداخلية، وتوفير أمن المعلومات، ومكافحة الاحتيال، وتحليل البيانات، والتواصل بين الفروع والأقسام المختلفة.

المطلب الأول: أهمية تقنية المعلومات

تستخدم تقنية المعلومات لتخزين المعلومات وحمايتها ومعالجتها وتأمينها وكذلك نقلها واستلامها واسترجاعها، حيث أنه يتم استخدامها في المؤسسات التجارية لحل المشكلات الرياضية والمنطقية، كما أنها تساعد في أنظمة إدارة المشاريع؛ حيث يتم أولاً التخطيط ومن ثم جمع البيانات وفرزها ومعالجتها وصولاً إلى إنشاء النتائج، وكذلك الأمر فإنّ تقنية المعلومات تساعد العمال ومدراءهم في الاستفسار عن مشكلة معينة وإدراك مدى تعقيدها، وكذلك في إنشاء منتجات وخدمات جديدة وبالتالي تحسين الإنتاجية والمردود.

وتقنية المعلومات تلعب دورًا حيويًا في الوقاية من الاحتيال لدى البنوك التجارية، وترجم أهميتها في عدة نقاط:

- تحسين التحقق والتحقيق: تقنية المعلومات تمكّن البنوك من تطبيق أنظمة التحقق الثنائي والتعرف البيومتري وغيرها من التقنيات المتقدمة للتحقق من هوية العميل وصحة المعاملات، مما يقلل من فرص ارتكاب الاحتيال.

- مراقبة الأنشطة المشبوهة: تتيح تقنية المعلومات للبنوك مراقبة الأنشطة المشبوهة واكتشاف الأنماط غير المعتادة في المعاملات، مما يسمح بالتدخل المبكر لمنع الاحتيال وتقليل الخسائر.

- تحليل البيانات والذكاء الاصطناعي: يمكن استخدام تقنية المعلومات لتحليل البيانات المالية واكتشاف الاتجاهات والنماذج غير العادية التي قد تشير إلى وجود احتيال، وذلك باستخدام تقنيات مثل التعلم الآلي وتحليل البيانات الضخمة.
 - تعزيز الأمن السيبراني: تلعب تقنية المعلومات دورًا حاسمًا في تطبيق الحماية السيبرانية للبنوك، بما في ذلك تأمين شبكات الاتصالات وتشفير البيانات وتطبيق السياسات والإجراءات الأمنية.
 - توفير الأدوات والأنظمة المتقدمة: تساهم تقنية المعلومات في توفير الأدوات والأنظمة المتقدمة التي تسهل عمليات الرصد والتحليل والتقييم المستمر لنشاطات الاحتيال وتطورها، وبالتالي تمكين البنوك من اتخاذ إجراءات فعالة لمكافحة.
- بشكل عام، يمكن القول إن تقنية المعلومات تعد عنصرًا أساسيًا في جهود البنوك للحفاظ على أمن وسلامة المعاملات المالية ومكافحة الاحتيال، مما يحقق الثقة لدى العملاء ويحافظ على سمعة البنك واستقراره المالي.

المطلب الثاني: آلية عمل تقنية المعلومات من الوقاية من الاحتيال لدى البنوك التجارية:

- آلية عمل تقنية المعلومات من الوقاية من الاحتيال لدى البنوك التجارية تتضمن عدة خطوات وتقنيات تعمل سويًا لتحقيق هذا الهدف، هناك عدة عناصر تشكل أساس هذه الآلية:
- التحقق الثنائي: يتضمن التحقق من هوية المستخدم بوسائل متعددة، مثل كلمات المرور والرموز السرية، ورسائل نصية تأكيدية، وبصمات الأصابع، والتعرف الصوتي. هذه الطرق تساهم في زيادة أمان الحسابات والمعاملات.
 - مراقبة السلوك الغير طبيعي: تقنيات تحليل السلوك العادي للعملاء تستخدم لاكتشاف الأنشطة غير المعتادة أو الغير متوقعة، مثل تسجيل الدخول من موقع غير معتاد أو إجراء معاملة بمبلغ كبير بشكل غير مألوف.
 - التحليل الضخم للبيانات: تقنيات التحليل الضخم تستخدم لتحليل كميات كبيرة من البيانات المالية وتحديد الأنماط غير المعتادة التي قد تشير إلى وجود احتيال، مما يساعد في الكشف المبكر والوقاية.
 - تقنيات الذكاء الاصطناعي والتعلم الآلي: تستخدم الذكاء الاصطناعي وتقنيات التعلم الآلي لتطوير نماذج تنبؤية قادرة على اكتشاف الاحتيال بناءً على البيانات التاريخية والسلوك الحالي.

- تحليل البيانات البيومترية: يتم استخدام تقنيات التعرف البيومترية، مثل البصمات الإصبعية والتعرف على الوجوه، لتعزيز عمليات التحقق من هوية العملاء والموظفين.
- تحسين أمان البنية التحتية الرقمية: يتم تعزيز أمان البنية التحتية الرقمية للبنوك بواسطة التشفير القوي، وجدران الحماية، والكشف عن التسلل، وأجهزة الرصد، لمنع الوصول غير المصرح به وحماية البيانات المالية. هذه العناصر والتقنيات تعمل سويًا كجزء من آلية شاملة للوقاية من الاحتيال في البنوك التجارية، حيث تساعد في رصد وكشف ومنع الأنشطة الاحتيالية بشكل فعال وفي الوقت المناسب.

المطلب الثالث: دور تقنية المعلومات في مكافحة عمليات الاحتيال

تلعب التكنولوجيا دوراً حاسماً في اكتشاف ومكافحة عمليات الاحتيال، ومع تزايد تعقيد وتطور عمليات الاحتيال هذه، لم تعد طرق الكشف اليدوية وحدها كافية، لقد وفر التقدم التكنولوجي أدوات وتقنيات قوية يمكن أن تساعد المؤسسات المالية ووكالات إنفاذ القانون في التعرف على عمليات الاحتيال الفاشلة ومكافحتها بشكل أكثر فعالية.

تحليلات البيانات المتقدمة والتعلم الآلي: أحد التطورات التكنولوجية الرئيسية في الكشف عن الاحتيال هو استخدام تحليلات البيانات المتقدمة وخوارزميات التعلم الآلي، تمكن هذه التقنيات المؤسسات المالية من تحليل كميات كبيرة من البيانات في الوقت الفعلي وتحديد الأنماط والشذوذات التي قد تشير إلى أنشطة احتيالية، ومن خلال الاستفادة من بيانات المعاملات التاريخية، يمكن لهذه الخوارزميات التعلم من حالات الاحتيال السابقة وتحسين دقتها بشكل مستمر في اكتشاف الحالات الجديدة.

المراقبة والتنبيهات في الوقت الحقيقي: تعد أنظمة المراقبة في الوقت الفعلي تقنية مهمة أخرى في مكافحة عمليات الاحتيال. تقوم هذه الأنظمة بمراقبة المعاملات وأنشطة الحساب بشكل مستمر، والإشارة إلى الأنماط أو السلوكيات المشبوهة لإجراء مزيد من التحقيق. على سبيل المثال، إذا تم الكشف عن زيادة مفاجئة في حجم المعاملات أو سلسلة من المعاملات ذات القيمة العالية، فيمكن إطلاق تنبيه، مما يدفع إلى اتخاذ إجراءات فورية لمنع الاحتيال المحتمل. توفر أنظمة المراقبة في الوقت الفعلي طبقة إضافية من الأمان وتتيح الاستجابة السريعة للتخفيف من الخسائر.

الذكاء الاصطناعي ومعالجة اللغات الطبيعية:

كما أثبتت تقنيات الذكاء الاصطناعي (AI) ومعالجة اللغات الطبيعية (NLP) أهميتها في مكافحة عمليات الاحتيال. يمكن للأنظمة التي تعمل بالذكاء الاصطناعي تحليل البيانات غير المنظمة، مثل رسائل البريد الإلكتروني وسجلات الدردشة ومنشورات وسائل التواصل الاجتماعي، لتحديد مؤشرات الاحتيال المحتملة. ومن خلال تحليل اللغة المستخدمة في الاتصالات، يمكن لهذه الأنظمة اكتشاف المحادثات المشبوهة أو محاولات الخداع. تساعد هذه التقنية في الكشف عن الاتصالات المخفية وتوفير رؤية قيمة حول أنشطة المحتالين.

تقنية البلوكشين: لقد اكتسبت تقنية Blockchain الاهتمام لإمكاناتها في مكافحة الاحتيال، بما في ذلك مخططات الإفلاس. من خلال إنشاء سجل للمعاملات مقاوم للتلاعب ولا شفاف، يمكن أن تساعد تقنية blockchain في منع الأنشطة الاحتيالية من خلال ضمان سلامة البيانات وعدم قابليتها للتغيير. يمكن للمؤسسات المالية الاستفادة من تقنية blockchain للتحقق بشكل آمن من هويات الأفراد أو الكيانات المشاركة في المعاملات، مما يقلل من مخاطر الأنشطة الاحتيالية المرتبطة بالشركات الوهمية أو الهويات المزيفة.

التعاون وتبادل المعلومات:

في المعركة ضد عمليات الاحتيال الهائلة، يعد التعاون وتبادل المعلومات بين المؤسسات المالية ووكالات إنفاذ القانون ومقدمي التكنولوجيا أمراً ضرورياً. ومن خلال تبادل الأفكار وأفضل الممارسات ومعلومات الاحتيال، يمكن لأصحاب المصلحة هؤلاء بشكل جماعي البقاء في صدارة المحتالين. وتعمل المنصات التعاونية وشبكات تبادل المعلومات على تمكين النشر السريع للتنبيهات والتحذيرات، مما يضمن أن تكون جميع الأطراف على اطلاع جيد ومجهزة لمكافحة عمليات الاحتيال الفاشلة بفعالية.

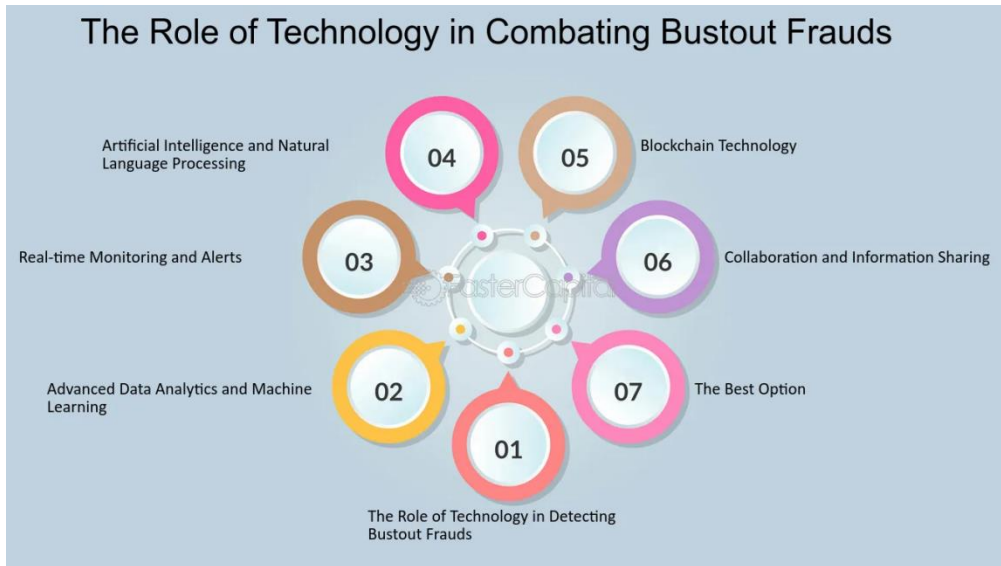
الخيار الأفضل: نهج متعدد الطبقات:

في حين أن كل من هذه التقنيات لديها نقاط قوتها، فإن النهج الأكثر فعالية لمكافحة عمليات الاحتيال هو نهج متعدد الطبقات. يوفر استخدام مزيج من تحليلات البيانات المتقدمة، والمراقبة في الوقت الفعلي، والذكاء الاصطناعي، ومعالجة اللغات الطبيعية، وتكنولوجيا blockchain دفاعاً شاملاً ضد الأنشطة الاحتيالية، ومن خلال دمج هذه التقنيات في البنية التحتية الحالية للكشف عن الاحتيال ومنعه، يمكن للمؤسسات المالية أن تعزز بشكل كبير قدرتها على اكتشاف وتخفيف عمليات الاحتيال.

تلعب التكنولوجيا دوراً حاسماً في مكافحة عمليات الاحتيال من خلال توفير أدوات وتقنيات قوية للكشف عنها ومنعها. تعد تحليلات البيانات المتقدمة، والمراقبة في الوقت الفعلي، والذكاء الاصطناعي، ومعالجة اللغات الطبيعية، وتقنية blockchain، كلها ذات قيمة لا تقدر بثمن في تحديد الأنماط المشبوهة، والكشف عن الاتصالات المخفية، وضمان سلامة المعاملات. ومن خلال اعتماد نهج متعدد الطبقات يستخدم هذه التقنيات، يمكن للمؤسسات المالية أن تتقدم بخطوة واحدة على المحتالين وتحمي نفسها وعملائها من العواقب المدمرة لعمليات الاحتيال الفاشلة.

شكل رقم (1)

دور تقنية المعلومات في مكافحة عملية الاحتيال



المبحث الثاني: الاحتيال

الاحتيال هو واحد من التحديات التي تواجه المنشآت المالية أو المصرفية، فهو يعيق الأداء ويهدر الأموال والموارد النادرة ويلحق الأذى بالمنشأة وبسمعتها وبقدرتها التنافسية، وقد يتخذ الضرر أشكالاً عدة غير الخسارة المالية بحد ذاتها مهما بلغت قيمتها. فالضرر الأكبر قد يكون ذلك الذي يلحق بأداء المنشأة وسمعتها ومصداقيتها وثقة السوق والجمهور بها وفي نهاية المطاف قد يؤدي إلى تعريضها لمخاطر متعددة.

والمشكلة كبيرة بكل المقاييس ويبدو أنها لا تقتصر على أي منشأة بعينها في القطاع الخاص سواء كانت منشأة مالية أو صناعية أو خدمية، إضافة إلى ذلك أن الاحتيال يتكيف مع المتغيرات التي قد تطرأ على أي قطاع، فبالرغم من آليات التدقيق الداخلي والمراقبة والتقصي وشروط مراجعي الحسابات الخارجيين المستقلين وقواعد السلوك المهني يستمر حدوث الاحتيال.

ويصعب في الغالب استرداد الأموال المهذرة بسبب نشاطات الاحتيال، وفي كثير من الأحيان يكون هذا الأمر مستحيلاً، لذلك تكون برامج مكافحة ومراقبة عمليات الاحتيال أقل كلفة وأكثر فعالية من محاولات استرداد تلك الأموال المختلسة.

وبالرغم من ذلك فإن هناك عدد من البنوك والمنشآت المالية قد تلجأ للتأمين الحماية نفسها ضد المخاطر التشغيلية الناتجة عن أحداث مثل الاختلاس والاحتيال المالي من قبل الموظفين، ومع ذلك فإنها لا تستطيع أن تعتمد كلياً على التأمين كوسيلة للتخفيف من المخاطر التشغيلية، فالتأخير في الدفع والطعون النظامية بالشروط التعاقدية تؤكد بأن التأمين لا يوفر التغطية المثالية، أضف إلى ذلك فإن النتائج السلبية للمطالبات المتصلة بالاحتيال ستؤدي إلى ارتفاع أقساط التأمين خاصة عندما تكون قوى السوق تتجه نحو تصعيد أسعار التأمين حتى للبنوك التي لها سجل جيد في مثل هذه العمليات.

المطلب الأول: تعريف الاحتيال:

التعريف البسيط للاحتيال هو أية ممارسة تنطوي على استخدام الخداع للحصول المباشر أو غير المباشر على شكل من أشكال الاستفادة المالية لمرتكب الجريمة، أو تسهيل ذلك لغيره لتؤدي إلى شكل من أشكال الخسارة للطرف الذي تعرّض للاحتيال. وغالباً ما تتصل الخسارة الفعلية الناتجة عن الاحتيال في البنوك بالموجودات السائلة مثل النقد والأوراق المالية .

وليس من الضروري أن يقتصر الاحتيال على المنافع النقدية والمادية، فتعريف الاحتيال الوارد في المراجع هو "التحريف المتعمد للحقيقة لأغراء أحدهم بالتنازل عن شيء ذي قيمة أو عن حق قانوني"، ويشمل هذا التعريف الكسب المالي إلى جانب منافع أخرى مثل حق الدخول أو الحصول على معلومات يمكن اكتسابها بالخداع أو بأي سلو له آخر غير شريف، وسواء كانت الخسارة مادية أو كانت تتصل بشيء غير ملموس مثل حقوق الملكية الأدبية، فغالبًا ما ينطوي الاحتيال على خسارة للبنك أو للمساهمين فيه أو للعملاء ومحاولة إخفاء ذلك الخسارة.

ويمكن أن يشمل الاختبار الأساسي للاحتيال الأسئلة التالية:

- هل هناك خداع للمنشأة؟
 - هل كان الفعل غير شرعي؟
 - هل نتج عن ذلك استفادة أو منافع مالية لصالح شخص لا يستحقها؟
 - هل تمت المحاولة للقيام بأي من ما ورد في الأسئلة السابقة؟
- ويجب التمييز بين الاحتيال من داخل البنك والاحتيال من خارج البنك، وتبين الدراسات التي أجريت على مؤسسات دولية باستمرار أن مرتكبي الاحتيال في معظم الأحوال هم من الموظفين، بمساعدة أو بدون مساعدة شركاء من الخارج، يدفعهم إلى ذلك عادة انتهاز الفرص والجشع والانتقام والحاجة لنقد سريع لدعم طراز معين من المعيشة ومشاكل مالية شخصية وعدم الرضا أو الولاء والضغط العائلي والحاجة التسديد الديون.
- وتتشابه البنوك من حيث ما تواجهه من احتيال في معظم دول العالم حيث أن معظم الخسائر تأتي نتيجة أعمال احتيالية من جانب الموظفين، وربما يشكل اختلاس النقود أكثرها شيوعًا، وبصورة خاصة اختلاس النقود والشيكات السياحية من الفروع ومكائن الصرف الآلي.

ولابد من الإشارة إلى أن حالات اختلاس النقد تنطوي على مبالغ غالبًا ما تكون زهيدة، في حين أن حالات الاحتيال عن طريق الدفع أو التحويل الإلكتروني أقل عددًا نسبيًا ولكنها تنطوي عادة على خسائر مالية أكبر.

ومن المعلوم تاريخيًا أن معظم الخسائر الناتجة من عمليات الاحتيال في البنوك تكون بسبب أشخاص يعملون لدى تلك البنوك في جميع المستويات الوظيفية، لذلك يتعين على أية استراتيجية تهدف إلى مكافحة الاحتيال أن تركز بصورة أساسية على ما يسمى بالاحتيال "في مكان العمل"، في الوقت ذاته، فإن مفهوم الاحتيال لا يجوز أن يتجاهل خطر الاحتيال الخارجي، أو ما يشار إليه أيضًا باحتيال العميل.

والاحتيال الخارجي يرتكبه أشخاص من خارج البنك (عادة ما يكونوا مجرمين محترفين) وغالبًا بمساعدة ومعرفة أشخاص من داخل البنك. ولفهم الاحتيال بصورة صحيحة، علينا أن ندرك أن أعمال الاحتيال يرتكبها أشخاص هم موضع ثقة، وهذا ما يفسر طول المدة في اكتشاف الاحتيال ولماذا عند اكتشاف المرتكب، يقر زملاؤه أن شكوكًا كانت تساورهم لبعض الوقت لكنهم كانوا يشعرون بعجزهم عن القيام بأي عمل قد يساعد على اكتشاف هذه العمليات في وقت مبكر.

ويمكن اعتبار الاحتيال كجزء هام جدًا، من القضية الأوسع المعروفة باسم الفساد. وينطوي الفساد بصورة عامة على أعمال غير صالحة أو اغفالات أو سوء استخدام النفوذ أو المراكز أو سوء استخدام المعلومات.

عينه من عمليات الاحتيال:

هناك عدة أمثلة من الاحتيال المصرفي منها:

- اختلاس النقد والموجودات الثمينة الأخرى.
- تزوير أو تحريف المستندات بما في ذلك طلبات التوظيف والفواتير والشيكات وشهادات الأهلية أو التأهيل أو مستندات الهوية أو بطاقات الصرف الآلي أو البطاقات الائتمانية.
- تزوير التوقييع والأختام .
- تزيف الأوراق النقدية.
- تغيير أحد أو كل أركان مكونات الشيك.
- سرقة بطاقات الصرف الآلي أو بطاقات الائتمان واستعمالها بطريق غير شرعية.
- إدخال تعليمات وبيانات غير سليمة من خلال الحاسب الآلي.
- سوء استخدام المعلومات وتسريبها بطرق غير شرعية.
- تحويل أموال لعملاء وهميين أو موظفين أو باعة.
- قبول الرشاوى أو الهدايا أو العمولات السرية لمنح عقد أو تجاهل الإجراءات المتخذة وحالات عدم الالتزام أو كدافع لتقديم منافع بما في ذلك الوصول إلى معلومات سرية.
- الحصول عن طريق الاحتيال على منافع أو مستندات لا يحق للمستلم أن يحصل عليها.

المطلب الثاني: دور التقنية:

أثبتت التقنية الحديثة في القطاع المصرفي أنها سلاح ذو حدين، فمن ناحية استفادت جهود مكافحة الاحتيال بشكل واضح من التقنية الحديثة إذ أن الانتقال من النظام النقدي إلى نقل الأموال إلكترونياً، على سبيل المثال، قد خفض من أخطار اختلاس النقود لانخفاض حيازة النقود، كما أن تطوير وسائل وأدوات لاكتشاف الاحتيال يعود الفضل فيه إلى التقنية المتطورة.

ولكن من ناحية أخرى فقد برع المحتالون باستخدام أحدث التقنيات لتعزيز قدراتهم، ويمكن القول أن لا شيء قد سهل الاحتيال أكثر من الانتشار الواسع لأجهزة الحاسب الألي زهيدة الثمن وعالية القدرة والمتوفرة بسهولة وما يتصل بها من تقنيات أخرى، فتقنيات المستندات الحالية مثل المسحات البصرية وطابعات الليزر والناسخات والبرامج المختلفة قد سمحت بأعمال تزوير يصعب جداً اكتشافها، فوسائل تزوير الشبكات البسيطة في السابق قد حل مكانها أعمال تزوير عالية الجودة لجميع الأوراق المالية القابلة للتداول بما في ذلك الشيكات وخطابات الاعتماد وأذونات الخزينة والسندات، وبما أن البنوك السعودية قد تقدمت كثيراً في الفترة الماضية في إدخال النظام التقني على أنظمتها من الأرجح أن ينخفض عدد أعمال تزوير المستندات، في حين أن مستوى التزوير التقني المتطور وقيمه النقدية سيصبح الأرجح.

كما أن التقنيات الحديثة قد سمحت بتزييف العملات وبطاقات الائتمان بشكل واسع، وهو نشاط معروف لدى عصابات الجريمة المنظمة، فعمليات تزييف العملات الرئيسية، بصورة خاصة، تمارس على المستوى الدولي بالتعاون مع عصابات غسل الأموال.

ولقد أدت التقنيات الحديثة، إضافة إلى خطر الاحتيال التقليدي المرتبط بعمليات (Insider Trading) إلى ارتفاع مخاطر التعرض للخسائر المالية، فعند قيام أحد موظفي البنك بتعديل حالة مديونية بصورة احتيالية أو عند قيام أحد الوسطاء بإجراء صفقات غير معتمدة أو بتجاوز حدود الصفقة فإن كل منهما يعرض البنك إلى خسائر مدمرة محتملة في فترة قصيرة من الوقت.

أن التحول إلى النشاط المصرفي عن طريق الانترنت يعرض البنوك كذلك إلى مخاطر جديدة، فالمحتالون مطلعون على أحدث التقنيات بعمق وعلى نقاط الضعف الكامنة في إجراءات الرقابة الداخلية لدى البنوك وهم يمثلون خطراً متنامياً من مخاطر الجريمة الالكترونية (Cyber Crime).

ومن غير المتوقع أن تواكب المعلومات حول الجريمة الالكترونية الواردة في هذه الإرشادات التقدم السريع للتطور التقني، لذلك يتوجب على البنوك أن تظل مطلعة على أحدث التطورات التقنية التي يستخدمها المحتالون وعلى أحدث الوسائل لاكتشاف ومراقبة ومكافحة الاحتيال، ولهذه الغاية ينبغي استمرار تطوير الأنظمة والإجراءات الداخلية لرصد وتحليل اتجاهات الاحتيال ووسائل مكافحته وإيجاز هذه المعلومات الهامة وتوزيعها على موظفي البنك، وتتضمن خطة مكافحة ومراقبة عمليات الاحتيال الواردة في هذه الإرشادات عددًا من الاقتراحات بهذا الشأن.

المطلب الثالث: خطة مكافحة الاحتيال:

من الضرورة أن يقوم كل بنك بوضع خطة متكاملة لمكافحة الاحتيال المعالجة جميع جوانب الاحتيال، وتترح هذه التعليمات تسعة شروط أساسية لتطوير خطة فاعلة لمكافحة الاحتيال لدى البنوك السعودية، وذلك بالاستناد إلى مراجعة واعتماد أفضل الممارسات الدولية في هذا المجال، وهذه الشروط الأساسية التسعة المقترحة هي كالتالي:

- الأول: استراتيجية مكافحة الاحتيال وسياسة الرقابة .
 - الثاني: الإطار التنظيمي وهيكلية المسؤولية .
 - الثالث: تقييم مخاطر الاحتيال .
 - الرابع: نشر الوعي بشأن الاحتيال.
 - الخامس: إجراءات المراقبة.
 - السادس: الرقابة والمتابعة.
 - السابع: أنظمة الإبلاغ عن الاحتيال.
 - الثامن: معايير التحقيق.
 - التاسع: معايير السلوك والتأديب
- هذه الشروط والتعليمات الإرشادية هي عامة لا تفصيلية تتضمن قائمة بالأمور التي تحتاج للمعالجة بعمق من قبل أي بنك حسب ظروفه الخاصة، وتقع على عاتق البنك مسؤولية تطوير الإجراءات والمعايير والأنظمة والعمليات اللازمة لتطبيق هذه الشروط بصورة فاعلة ومتابعتها كجزء من حملة مستمرة يشنها البنك بكامله لمكافحة الاحتيال.

جوهر أسلوب مكافحة الاحتيال هو الاقتناع بأهمية إدارة المخاطر، فباستخدام تقنيات الإدارة تستطيع أن تحدد بوضوح معظم نقاط الضعف في الضوابط وأن تتخذ التدابير اللازمة لإصلاح آليات المراقبة الضعيفة أو إدخال تقنيات إضافية.

تناقش الأجزاء التالية الشروط الأساسية التسعة كل على حده بحيث يبدأ كل جزء بمقدمة عامة موجزة تلها إرشادات محددة تهدف إلى مساعدة البنوك في جهودها لمعالجة احتياجاتها الخاصة.

الشرط الأساسي الأول: استراتيجية معقمة الاحتيال وسياسة الرقبة:

يتعين على كل بنك أن يكون لديه سياسه مكتوبه شاملة ومتكاملة لمكافحة الاحتيال ومراقبته مع تفاصيل المراقبة لمكافحة الاحتيال والفساد، ويجب أن ترسم هذه السياسة كافة التدابير والإجراءات الصالحة للبنك المعين، إلى جانب سلسلة واسعة ومكاملة من التدابير المضادة للاحتيال، ويجب أن تتبنى هذه السياسة أسلوب إدارة المخاطر لمكافحة ومراقبة الاحتيال، كما يجب أن يكون الغرض الرئيسي لهذه السياسة هو نشر الوعي والالتزام بين الموظفين، وان تحدد من هو المسؤول في البنك عن مكافحة ومراقبة الاحتيال وعن تطبيق مختلف جوانب خطة مكافحة ومراقبه الاحتيال، ومن أجل تقييم فعالية الخطة يجب أن تخضع هذه الخطة للمتابعة والتقييم من الداخل والخارج.

الإرشادات:

1. على البنك أن يضع سياسة مكتوبة لمكافحة الاحتيال ومراقبته ويتم توزيعها على موظفيه.
2. تتضمن هذه السياسة مراقبة البنك للاحتيال ومكافحه الفساد وأن تضع الأهداف وأن تجمع السياسات القائمة والإجراءات التي تتصل بمكافحة الاحتيال والفساد.
3. يمكن أن ترد السياسة في وثيقه واحدة أو في مجموعه من الكتيّبات والتوجيهات والتعاميم والإرشادات توضح بمجملها عناصر استراتيجية البنك.
4. تقوم السياسة على أساس تحليل مخاطر البنك من حيث بيئته الداخلية والخارجية وأن تتبنى أسلوب إدارة المخاطر بشأن مراقبة الاحتيال (يغطي هذا الجانب الشريط الأساسي الثالث بعنوان "تقييم خطر الاحتيال").
5. تكون السياسة شاملة وأن تغطي العناصر الحيوية للبنك ونشاطاته.

6. تكون السياسة متكاملة دون أي تضارب بين العناصر المستقلة.
7. تحدد سياسة مكافحة الاحتيال بالتفصيل أعضاء لجنة مكافحة الاحتيال ونطاق عملها وأغراضها. المؤلفه من موظفين رئيسيين من مختلف أقسام البنك مسئولة عن تطوير تلك السياسة وتطبيقها وتنسيقها.
8. على المسؤولين التنفيذيين أن يكونوا القدوة بالتصرف بنزاهة والتقيد بروح ونصوص سياسة مكافحة الاحتيال ومراقبته، كما يجب أن يدركوا بأنهم مسئولين وخاضعين للمحاسبة في إيجاد مناخ أخلاقي والمحافظة عليه مما يؤدي إلى إحباط الاحتيال وتشجيع الإبلاغ عن أي خرق للمعايير المقبولة.
9. رصد ما يكفي من العناصر البشرية والموارد الأخرى لضمان نجاح سياسة مكافحة ومراقبة الاحتيال، فالالتزام الواضح من كبار المسئولين من حيث الوقت ورصد الموارد، يساعد في إرسال إشارة واضحة إلى الموظفين بان الإدارة لن تتهاون في مكافحة الفساد.
10. على جميع الموظفين أن يعوا مسؤولياتهم المتعلقة بمكافحة الاحتيال والكشف والإبلاغ عنه والتحقيق بشأنه.
11. أنه من الملائم إشراك الجهاز التشغيلي في وضع صيغة سياسة مكافحة الاحتيال لتحديد أين توجد فرص الفساد وكيف يمكن تقليصها للحد الأدنى.
12. من الأهمية بمكان إطلاع الجهاز التشغيلي باستمرار على تطورات السياسة وتطبيقها والإنجازات والمنافع لتعزيز الالتزام بأغراض تلك السياسة على أوسع نطاق.
13. يساعد العمل الجماعي ونشر الثقافة التنظيمية البنوك على الاستفادة من الخبرات والأفكار المجمعة.
14. تكيف وتحديث سياسة مكافحة ومراقبة الاحتيال بحيث تعكس التغيرات في البنك وفي بيئته التشغيلية، ولهذا الغرض يتم مراجعة السياسة دوريًا كل سنتين مثلاً أو عند حدوث تغييرات في البيئة التشغيلية تؤدي الإضعاف قدرة تلك السياسات على مكافحة ومراقبة الاحتيال وأيضاً لاستعراض قدرتها على تلبية الأغراض المعاد تقيمها.

الشرط الأساسي الثاني: الإطار التنظيمي وهيكلية المسؤولية:

يجب تطوير إطار تنظيمي شامل وفعال وهيكلية مسؤوليات لتنفيذ سياسة مراقبة الاحتيال الشاملة التي يعتمد عليها البنك، يتضمنها تنفيذ أنظمة مراقبة داخلية سليمة، وينبغي تكوين لجنة لمراقبة الاحتيال لوضع

السياسة وتنسيق ومتابعة تنفيذها وتوفير المساندة اللازمة لها، وإشراك جميع مستويات الإدارة في تنفيذ هذه السياسة.

الإرشادات:

1. تحديد المسؤولية التنظيمية لاستراتيجية البنك الشاملة لمكافحة الاحتيال ولكل عنصر من عناصرها بكل وضوح وإبلاغ إدارة البنك وموظفيه بكل ذلك.
2. ينبغي أن تكون هناك لجنة مستقلة معنية بمكافحة ومراقبة الاحتيال لدى البنك، ما نوصي بالأمور التالية:
 - تكون مهمة لجنة مراقبة الاحتيال في وضع وتنسيق ومتابعة سياسة الكشف عن الاحتيال والتحقيق بشأنه.
 - تحديد مسؤولية مراقبة الاحتيال بكل وضوح.
 - تنفيذ هيكلية واضحة للإبلاغ عن الاحتيال.
3. توثيق أدوار ومسؤوليات جميع الموظفين بوضوح في سياسة مكافحة ومراقبة الاحتيال، على كل موظف أن يعرف بمن يتصل وما يجب عليه فعله عند الاشتباه بنشاط احتيالي.

مسؤوليات الإدارة :

1. الإدارة هي مسئولة عن مكافحة الاحتيال. لذلك تكتمل الإدارة بشكل تام مسؤولية وضع وتحديد المسؤولية التنظيمية لمكافحة الاحتيال ومنعه.
2. تدل الدراسات الصادرة عن الشركات العالمية للاستشارات الإدارية أن سلوك كبار التنفيذيين في البنك، هو من أهم جوانب خلق مناخ أخلاقي في أي منشأة يجب أن يبدأ السلوك الصحيح من قمة الهرم وينتقل نزولاً إلى القاعدة عبر تصريف كبار المسؤولين بنزاهة وممارسة ما ينادون به، ونظراً لأن سلوك الموظف ومواقفه داخل المنشأة المالية الكبرى تتأثر كثيراً بالإدارة العليا، لذا يتعين على المدراء أن يكونوا القدوة بإتباعهم إجراءات الرقابة الصحيحة في أعمالهم اليومية وعدم خرق الإجراءات النظامية بحكم موقعهم.
3. كما تدل الدراسات على أنه كلما كان المدراء التنفيذيين على فهم وثيق بالعمليات المصرفية، كلما انخفضت حوادث الاحتيال التي يتعرض لها البنك، وبما أن سلوك الموظف ومواقفه داخل المنشأة المالية الكبرى يتأثر

كثيراً بالإدارة العليا، لذا يتعين على المدراء أن يكونوا القدوة بإتباعهم إجراءات الرقابة الصحيحة في أعمالهم اليومية وعدم خرق الإجراءات النظامية بحكم مواقعهم.

4. على المدراء أن يعوا مسؤولية الولاء لمركزهم في الكشف عن الاحتيال ومكافحته، ومن المهم توثيق مسؤوليات الإدارة عن كشف الاحتيال ومكافحته على مستوى استراتيجي في خطط الإدارة وكتيبات التشغيل.

5. على المستوى التشغيلي، تحدد مسؤولية الإدارة عن كشف الاحتيال ومكافحته في أوصاف الوظيفة وتعاميم وإجراءات المركز والفروع.

6. على المدراء أن يوفرُوا التوجيه اللازم والمساندة للموظفين حول الإبلاغ عن الاحتيال المشتبه به، فإذا بلغ الموظفون عن ممارسات غير نزيهة ولم يتلقوا بعدها المساندة اللازمة من الإدارة تفقد سياسة الرقابة على الاحتيال مصداقيتها.

7. يتمتع المسئول عن مكافحة الاحتيال بمسؤوليات تمكنه من القيام بعمله على نطاق البنك، وليس من الضروري تولي هذه المهمة كوظيفة مستقلة بل يمكن تكليف أحد العاملين في البنك بالقيام بهذه المهمة إضافة إلى أعماله شريطة عدم التعارض بين المسؤوليات، لكن من الضروري أن يعطى الشخص المعين لهذه المهمة الصلاحية الكافية للتعامل مع الاحتيال بصورة فاعلة، ويجب في بعض الحالات أن يكون للمسئول عن الاحتيال حق الاتصال المباشر بالمستويات العليا للبنك.

المطلب الرابع: لجنة مراقبة الاحتيال:

تلعب لجنة مراقبة الاحتيال لدى البنك دوراً رئيسياً في وضع السياسة والتثبيت من أن السياسات والإجراءات والتدابير التي تتضمنها الاستراتيجية الشاملة لمراقبة الاحتيال يتم تطبيقها بصورة فعالة، وتشرف اللجنة على تطوير عناصر الشروط الأساسية التسعة لمكافحة ومراقبة الاحتيال.

إنشاء لجنة مكافحة الاحتيال لوضع السياسة وتنسيق ومتابعة تنفيذها وتقديم المساندة للرئيس التنفيذي، على ألا تكون مهمة مكافحة ومراقبة الاحتيال محصورة بهذه اللجنة، بل يجب أن تشترك جميع مستويات الإدارة والموظفين بالطرق الصحيحة في تنسيق سياسة مكافحة ومراقبة الاحتيال ومتابعتها باستمرار والترويج لها.

تحدد سياسة مكافحة الاحتيال لدى البنك أعضاء اللجنة ومسؤولياتها، تشمل اللجنة كبار المسؤولين الذين يمثلون العمليات الرئيسية في البنك.

تجتمع اللجنة بشكل دوري، وشهريًا إذا أمكن، ولكن مرة واحدة، على الأقل كل ثلاثة شهور، وأن يكون هناك إمكانية عقد اجتماعات طارئة للبحث في حالات الاحتيال الخطيرة المشتبه بها.

5. من مهام اللجنة الرئيسية الإبلاغ عن الاحتيال ومساندة الرئيس التنفيذي بشأن جميع جوانب سياسة البنك لمكافحة الاحتيال.

وحدة التحقيق بشأن الاحتيال:

دور وحدة تحقيق بشأن الاحتيال هو تقصي حالات الاحتيال المحتملة ضد البنك، وتشمل هذه المسؤولية جمع وتقديم الأدلة اللازمة لمساندة الإجراءات الإدارية أو التأديبية أو غيرها من الإجراءات والملاحقة القضائية ومحاولة استرداد الأموال موضع الاحتيال.

إضافة إلى ممارسة مهمة التحقيق، على وحدة التحقيق أن تقدّم ما يلي:

- المساعدة والمعلومات والنصح إلى لجنة مراقبة الاحتيال.
- المساعدة في تعزيز اكتشاف ومكافحة الاحتيال ونشر الوعي بشأنه.
- المساعدة والتوجيه بشأن التدريب على مكافحة الاحتيال.
- تقارير إلى قاعدة معلومات الاحتيال لدى مؤسسه النقد بصفة دورية حسب تعليماتها.
- تقارير دورية للإدارة التنفيذية عن حالات الاحتيال.
- تقارير فنية بالتوصيات لسد الثغرات في أنظمة الرقابة الداخلية، وادلة السياسات والإجراءات.
- إبلاغ ورفع مطالبات لتعويض عن الخسائر الناتجة من حالات الاحتيال لشركات التأمين.
- إنشاء قاعدة معلومات حول الاحتيال لاستخدامها من قبل وحدة مكافحة الاحتيال، لذلك قد تكون هذه الوحدة أصلح مجموعة في البنك للاحتفاظ بقاعدة المعلومات، وقد تقرر الإدارة التنفيذية أن تضع المسؤولية عن هذه المهمة في مكان آخر داخل البنك.
- تشكل قاعدة المعلومات أداة هامة لكشف ومكافحة الاحتيال ولإدارة سياسة البنك لمراقبة الاحتيال، وينبغي، في سبيل المحاسبة وتسهيل المرجعية، أن تتضمن قاعدة المعلومات كل التفاصيل عن الاحتيال الفعلي والمشتبه به.

تشمل قاعدة معلومات الاحتيال، كحد أدنى، التفاصيل التالية عن كل حالة احتيال:

- رقم مرجع (مرتبط بالسجلات المالية ذات الصلة).

- الوضع الراهن ما إذا تم إقفال الملف أو ما زال نشطاً.
- المعلومات ذات الصلة والتواريخ أو الفترة التي جرى الاحتيال خلالها.
- اسم أو أسماء المحتالين والأشخاص ذوي العلاقة سواء من موظفي البنك أو من خارجه.
- تقدير لقيمة الاحتيال المالية والأثر الشامل أو الأهمية الشاملة للاحتيال على عمليات البنك أو أدائه.
- الموقع الجغرافي أو المادي للاحتيال.
- طبيعة أو نقطة تركيز الاحتيال.
- الإجراءات التي تمت فيما يتعلق بالتحقيق.
- نتائج الاستقصاء.

المطلب الخامس: تحليل الاحتيال:

وضع قاعدة معلومات مصانة وموحدة لكافة حالات الاحتيال، ومراجعة الوضع الراهن لجميع حالات الاحتيال المبلغ عنها، ومراجعة حالات الاحتيال المبلغ عنها، وتحديد تفاصيل ونقاط ضعف الضوابط الداخلية والإجراءات والعمليات، وتحليل الاتجاهات وتحديد الأسباب وتقييم الحوادث بطريقة نظامية.

التوعية:

- تحديد احتياجات وبرامج التدريب الصالحة لتوعية الموظفين بشأن الاحتيال.
- الإشراف على برامج التثقيف والتوعية بشأن الاحتيال.
- الاطلاع المستمر على تطورات وقضايا مراقبة الاحتيال بوجه عام وتوزيع معلومات الممارسات الأفضل عبر النشرات ووسائل الاتصال الأخرى حول الاحتيال في جميع أقسام البنك.

التحقيق بشأن الاحتيال:

- تحديد سياسة كيفية معالجة الاحتيال وتقديم النصح والمساعدة للوحدات العاملة في التحقيق.
- إجراء عمليات التقييم الأولية لجميع حالات الاحتيال المؤكدة.
- المصادقة على الإجراءات التأديبية (مع أنه يمكن حدوث ذلك بطرق أخرى).

الإبلاغ:

- التأكد من الإبلاغ عن جميع حالات الاحتيال في الوقت المناسب وباستمرار، وهذا يشمل كافة المعلومات مثل الفروع المحلية والخارجية والحوادث الداخلية والخارجية والاحتيال الفعلي والمحتمل أو المشتبه به.
- تقديم التقارير الإحصائية إلى الإدارة.
- رفع التقارير ومحاضر جلسات اللجنة إلى لجنة مراجعة إدارة المخاطر.
- رفع التقارير إلى لجنة تدقيق الحسابات حول قضايا الاحتيال وتطبيق الاستراتيجيات الواردة في خطة مراقبة الاحتيال.

الدراسات السابقة:

الدراسات العربية:

دراسة السهلاوي (2018) تأثير المخاطر المالية على ربحية البنوك التجارية المدرجة في سوق الأسهم السعودي: دراسة قياسية.

هدفت هذه الدراسة إلى تحديد أثر المخاطر المالية في ربحية بنوك المملكة العربية السعودية، وذلك للفترة 2013-2017، ولتحقيق تم جمع البيانات اللازمة عن البنوك المدرجة في سوق الأسهم السعودي "تداول". شملت عينة الدراسة 12 بنك سعودي. وتم قياس الربحية بالمتغير التابع المتمثل في العائد على حقوق الملكية، والمتغيرات المستقلة المتمثلة في مؤشر مخاطر الائتمان ومؤشر مخاطر السيولة ومؤشر مخاطر رأس المال. واختبر نموذج الدراسة بيانات سلسلة زمنية وقطاعية للبنوك المدروسة، وتم ذلك باستخدام نموذج الانحدار وفق الأثر الثابت ونموذج الانحدار وفق الأثر المتغير. وتوصلت الدراسة إلى وجود علاقة سلبية ضعيفة بين مخاطر الائتمان والعائد على حقوق الملكية، ووجود علاقة طردية ضعيفة لمخاطر السيولة والعائد على حقوق الملكية، ووجود علاقة عكسية قوية لمخاطر رأس المال والعائد على حقوق الملكية.

الدراسات الأجنبية:

دراسة Retnoningrum Hidayah (2018) بعنوان:

FRAUD PREVENTION: INFORMATION TECHNOLOGY AND INTERNAL CONTROL PERSPECTIVE

منع الاحتيال: منظور تكنولوجيا المعلومات والرقابة الداخلية

تناول الباحث تعريف الاحتيال هو شكل من أشكال المرض الموجود في الكيان. ويتسبب الاحتيال في العديد من الخسائر المادية وغير المادية. ولذلك يجب منع الأعمال الاحتيالية لتحقيق جامعة جيدة الحكم، وهدفت هذه الدراسة إلى معرفة أثر تكنولوجيا المعلومات والرقابة الداخلية على الوقاية من الاحتيال في الجامعات، وتكونت عينة البحث من 90 فرداً. أداة التحليل المستخدمة هي WARP PLS 6.0، تستخدم تقنية أخذ العينات في هذه الدراسة أخذ العينات الملائمة. لقد وجدنا أن تكنولوجيا المعلومات تؤثر على الرقابة الداخلية، وأن الرقابة الداخلية لها تأثير على منع الاحتيال. ووجدنا أيضاً أن تكنولوجيا المعلومات تؤثر على منع الاحتيال. ومن هنا يتعين على الجامعة تحسين قدرتها في مجال تكنولوجيا المعلومات والرقابة الداخلية. يساهم البحث في أدبيات منع الاحتيال من خلال توفير رؤية قيمة حول أنظمة الرقابة الداخلية. يجب أن تضيف الأبحاث المستقبلية متغيرات أخرى حتى تكون النتائج أكثر شمولاً.

الجزء الثالث

الدراسة العملية واجراءاتها المنهجية.

المنهجية وطرق البحث

قام الباحث بإتباع المنهج الوصفي التحليلي كما يلي:

- المنهج الوصفي: حيث قام الباحث بعرض الظواهر كما هي موجودة في الواقع، وعرض جميع العوامل والمتغيرات التي تلعب دوراً أساسياً فيها.
- المنهج التحليلي: حيث يتم تحليل المعلومات التي جمعها الباحث من مصادرها المكتبية والميدانية، ووضع الحلول المناسبة لها.

مجتمع الدراسة والعينة:

يشمل مجتمع الدراسة عينة من العملاء المتعاملين مع البنوك التجارية المختلفة في المملكة.

عينة الدراسة: بلغ عددهم (50) عميل من عملاء المصارف التجارية بالمملكة، وكانت العينة عشوائية بسيطة.

متغيرات الدراسة:

المتغيرات المستقلة: هي المتغيرات الشخصية المتمثلة في: العمر، المؤهل العلمي، الجنس، عدد سنوات العمل، الحالة الاجتماعية، الراتب.

المتغير التابع: فاعلية تقنية المعلومات في الوقاية من الاحتيال.

أسلوب وأداة جمع البيانات:

تم تجميع البيانات الأولية الخاصة بموضوع الدراسة من خلال تصميم استبيان الكتروني قمنا بإعداده لأغراض الدراسة والمرفق صورة منه في الملحق رقم (١) وذلك بعد الاطلاع على استبيانات لدراسات سابقة، ويتكون الاستبيان من جزئين تخدم موضوع الدراسة وهي كالتالي:

الجزء الأول: ويشمل خمس أسئلة مغلقة ومرتبة، والتي تتعلق بمعرفة الخلفية الديموغرافية لمختلف أفراد العينة وهي تختص بالبيانات الشخصية للمستقصي منها كالعمر، المؤهل العلمي، وعدد تعامله مع المصارف التجارية بالمملكة.

الجزء الثاني: ويهدف إلى التعرف على آراء واتجاهات مفردات مجتمع الدراسة حول أسئلة الاستبيان الإلكتروني الذي تناول فاعلية تقنية المعلومات في الوقاية من الاحتيال في البنوك التجارية السعودية، وقد تم توزيع استبيان يشتمل على (15) عبارات مقسمة إلى (3) محاور بناء على بعض المعلومات المستخلصة من الكتب والرسائل العلمية.

- المحور الأول: وقيس واقع فاعلية تقنية المعلومات في البنوك التجارية، وتغطيه العبارات (من ١ إلى 5).
- المحور الثاني: يقيس مدى مساهمة تقنية المعلومات في الوقاية من الاحتيال، وتغطيه العبارات (من 6 إلى 10).
- المحور الثالث: وقيس مدى تأثير تقنية المعلومات في الوقاية من الاحتيال بالبنوك التجارية السعودية، وتغطيه العبارات (من 11 إلى 15).

وبعد الانتهاء من إعداد الاستبيان، قمنا بإجراء التعديلات المطلوبة وبما يخدم أغراض الدراسة وتم تحديد الاجابة من خلال مقياس ليكرت والذي يتدرج من (موافق - موافق بشدة - لا أوافق - لا أوافق بشدة) وبعد توزيع عينة استطلاعية قمنا بالتعديل على الاستبيان بما يتناسب مع بيئة مجتمع الدراسة، وبعد تحليل الاستمارات قمنا بدمج (أوافق بشدة مع موافق، ودمج غير أوافق بشدة مع لا أوافق) بما يتماشى مع طبيعة المجتمع الذي تمثله العينة.

الطرق الإحصائية المستخدمة

- 1- الإحصاءات الوصفية للمتغيرات الشخصية.
- 2- حساب الثبات والصدق للاستبانة ومحاورها.
- 3- الإحصاءات الوصفية للأسئلة التي على شكل مقياس ليكرت.

أساليب المعالجة الإحصائية:

تم استخدام في معالجة بيانات الدراسة الأساليب الإحصائية المناسبة لطبيعة الدراسة، وطبيعة بناء الأداة ومعاييرها، وذلك على النحو التالي:

1. التكرارات والنسب المئوية لوصف عينة الدراسة حسب المتغيرات الشخصية.
2. المتوسط الحسابي، والانحراف المعياري والترتب لمعرفة الرأي السائد لمفردات العينة حول عبارات الأداة.
3. معامل ألفا كرونباخ لتحديد معامل الثبات والاتساق الداخلي، لأداة الدراسة.

4. معامل ارتباط بيرسون "Pearson" لتحديد الصدق لأداة الدراسة، ولحساب معامل الارتباط بين محاور الدراسة.

أولاً: الإحصاءات الوصفية للمتغيرات الشخصية

في هذا البند توجد دراسة لتوزيع مفردات العينة حسب فئات المتغيرات الشخصية، ومن ثم الحصول على تكرارات في هذه الفئات وبالتالي النسبة المئوية لهذه التكرارات.

1- العمر:

جدول رقم (1)

التوزيع التكراري والنسبي لعينة الدراسة حسب العمر

العمر	التكرار	النسبة %
من ٢٠ إلى أقل من 25	5	10
من ٢5 إلى أقل من 30	17	34
من 3٠ إلى أقل من 35	12	24
من 35 فأكثر	16	32
المجموع	50	100

بناءً على جدول رقم (1) وجد الباحث أن 10% من العينة كانت أعمارهم من ٢٠ إلى أقل من ٢٥، و ٣4% كانت أعمارهم من ٢٥ إلى أقل من ٣٠، و ٢4% من العينة كانت أعمارهم من ٣٠ إلى أقل من ٣٥، بينما ٣2% كانت أعمارهم من ٣٥ فأكثر، واتضح من ذلك أن النسبة الأكبر من العينة تتراوح أعمارهم من ٢٥ إلى أقل من 30.

2. المؤهل العلمي:

جدول رقم (2)

التوزيع التكراري والنسبي لعينة الدراسة حسب المؤهل العلمي

المؤهل العلمي	التكرار	النسبة %
ثانوي	3	6
بكالوريوس	40	80
ماجستير	7	14
المجموع	50	100

بناءً على جدول رقم (2) وجد الباحث أن ٦% من العينة مؤهلهم العلمي ثانوي، في حين أن 80% لديهم درجة البكالوريوس، و١٤% لديهم درجة الماجستير، واتضح من ذلك أن الغالبية العظمى من العينة مؤهلهم العلمي بكالوريوس.

3. عدد سنوات التعامل مع المصارف التجارية:

جدول رقم (3)

التوزيع التكراري والنسبي لعينة الدراسة حسب عدد سنوات التعامل مع المصارف التجارية

عدد سنوات التعامل مع المصرف	التكرار	النسبة %
من سنة إلى أقل من ٥ سنوات	25	50
من 5 سنوات إلى أقل من 10 سنوات	12	24
من 10 سنوات إلى أقل من 15 سنة	7	14
من 15 سنة فأكثر	6	12
المجموع	50	100

من جدول رقم (3) لاحظ الباحث أن ٥0% من العينة كانت عدد سنوات تعاملهم مع المصارف التجارية ما بين سنة إلى أقل من ٥ سنوات، بينما ٢4% من ٥ إلى أقل من ١٠ سنوات، في حين أن 14% من أفراد العينة كان تعاملهم مع المصرف من ١٠ إلى أقل من ١٥ سنة، و١2% من ١٥ سنة فأكثر، وبناءً على ذلك اتضح أن نصف مجتمع الدراسة تقريباً كان تعاملهم مع المصارف التجارية السعودية تقريباً ما بين السنة والخمس سنوات.

ثانياً: صدق وثبات أداة جمع البيانات

تعتبر مرحلة اختيار وتصميم أداة جمع بيانات مناسبة لهدف ومجتمع الدراسة من أصعب مراحل البحث العلمي، وعادة ما يعتمد الباحث على عدة أسس عند اختياره أداة من بين الأدوات المتاحة له في عملية جمع البيانات، ومن أهم هذه الأسس هي مدى صدق وثبات البيانات التي توفرها الأداة؛ ذلك لأن ضعف صدق أو ثبات الأداة يؤدي بالضرورة إلى ضعف صحة وسلامة نتائج الدراسة بأكملها، لذلك يحرص الباحثين على اختيار الأداة ذات الصدق والثبات العاليين، من هذا المنطلق يتعين علينا معرفة مدى صدق وثبات أداة جمع البيانات.

1. الصدق: يقصد بصدق المقياس (Instrument Validity) إلى أي درجة يقيس المقياس الغرض المصمم من أجله، وعليه يمكن تعريف صدق أداة جمع البيانات إلى أي درجة توفر الأداة بيانات ذات علاقة بمشكلة

الدراسة من مجتمع الدراسة، أي أن الصدق يقصد به أن المقياس يقيس ما وضع لقياسه، أي يقيس السمة أو الظاهرة التي وُضع لقياسها ولا يقيس غيرها.

2. **الثبات:** من الصفات الأساسية التي يجب توافرها أيضًا في أداة جمع البيانات قبل الشروع في استخدامها هي خاصية الثبات، تكمن أهمية قياس درجة ثبات أداة جمع البيانات في أهمية الحصول على نتائج صحيحة كلما تم استخدامه، ويعرف ثبات المقياس إلى أي درجة يعطي المقياس قراءات متقاربة عند كل مرة يستخدم فيها، وبمعنى آخر فإن الثبات يعني استقرار المقياس وعدم تناقضه مع نفسه، أي أن المقياس يعطي نفس النتائج تقريبًا إذا أعيد تطبيقه على نفس العينة.

طرق حساب الثبات: يقاس ثبات أداة جمع البيانات بطرق مختلفة من بينها:

طريقة كرونباخ ألفا:

وهي من الطرق الشائعة الاستعمال لحساب معامل الثبات وتعتمد على معادلة رياضية تعالجها حزم البرامج الإحصائية لتحديد قيمة معامل "كرونباخ ألفا" وتكون محصورة بين صفر وواحد، وكلما كانت القيمة قريبة من الواحد دل ذلك على ثبات المقياس.

وقد تم استخدام معامل "كرونباخ ألفا" في حساب معامل الثبات، وتم الحصول على النتائج التالية:

جدول رقم (4)

معاملات الثبات للمحاور وللاستبيان ككل

المحاور	عدد العبارات	ألفا كرونباخ
واقع فاعلية تقنية المعلومات في البنوك التجارية	5	0,759
مدى مساهمة تقنية المعلومات في الوقاية من الاحتيال	5	0,663
مدى تأثير تقنية المعلومات في الوقاية من الاحتيال بالبنوك التجارية السعودية	5	0,820
الاستبيان ككل	15	0,836

مما يدل على ثبات المقياس، أن قيمة ألفا كرونباخ هنا قريبة من الواحد للمقياس ككل، وأكبر من ٠,٧٠ لبعض المحاور.

ولدراسة مدى اتساق عبارات هذه المحاور مع بعضها البعض وكذلك حساب مقياس الصدق قام الباحث بالتالي:

- 1- أخذ العبارة الأولى من كل محور وحذفها، ومن ثم حساب " ألفا كرونباخ " لباقي عبارات المحور.
- 2- إذا كانت قيمة "ألفا" بعد حذف العبارة أكبر من قيمة "ألفا" للمحور ككل فهذا يعني أن حذف العبارة يزيد من قيمة "ألفا" وبالتالي يجب حذف هذه العبارة لأنها تعتبر غير متسقة مع باقي العبارات.
- 3- أما إذا كانت قيمة "ألفا" بعد حذف العبارة أصغر من قيمة "ألفا" للمحور ككل فهذا يعني أن حذف العبارة يقلل من قيمة "ألفا" وبالتالي يجب إبقاء هذه العبارة، وتعتبر عبارة متسقة مع باقي عبارات المحور.
- 4- تكرار العملية السابقة لكل عبارة من عبارات كل محور، وإبقاء العبارات المتسقة مع بعضها البعض، وقد تم استخدام هذه الطريقة والحصول على النتائج التالية بعد حذف العبارات غير المتسقة من كل محور إن وجدت.

المحور الأول: واقع فاعلية تقنية المعلومات في البنوك التجارية

جدول رقم (5)

معاملات الاتساق والصدق لمحور واقع فاعلية تقنية المعلومات في البنوك التجارية

عبارات المحور	ألفا كرونباخ *	معامل الارتباط **
تقنية المعلومات تساهم في تحسين أمان المعاملات في البنوك التجارية.	0.694	0.586
البنوك التجارية تستخدم تقنية المعلومات بشكل فعال لتحليل البيانات المالية.	0.729	0.491
تقنية المعلومات توفر وسائل فعّالة لتحقيق التواصل بين الفروع والمؤسسات المالية.	0.723	0.504
تقنية المعلومات تعزز كفاءة إدارة العمليات والخدمات في البنوك التجارية.	0.694	0.585
تقنية المعلومات تساهم في تطوير حلول متقدمة لمكافحة الاحتيال وضمان سلامة العمليات المالية.	0.655	0.515
المحور ككل	0,759	

ملاحظة عامة:

* قيمة ألفا كرونباخ بعد حذف العبارة.

** قيمة الارتباط بين العبارة ومجموع العبارات وهو يقيس قيمة الصديق الداخلي أو ما يسمى صديق المحك.

لاحظ الباحث من الجدول أن قيم "ألفا كرونباخ" داخل الجدول أصغر من قيمة "ألفا كرونباخ" للمحور، وهذا يعني أن جميع العبارات داخل المحور متسقة مع بعضها البعض، كما أن معاملات الارتباط دالة معنويًا عند مستوى 0.01 ويقصد بذلك العلاقة بين درجة العبارة والدرجة الكلية وهذا يعني صديق عبارات المقياس لهذا المحور.

المحور الثاني: مدى مساهمة تقنية المعلومات في الوقاية من الاحتيال.

جدول رقم (6)

معاملات الاتساق والصديق لمحور مدى مساهمة تقنية المعلومات في الوقاية من الاحتيال

عبارات المحور	ألفا كرونباخ *	معامل الارتباط **
تقنية المعلومات تسهم في تحديد الأنماط الغير معتادة في المعاملات المالية للوقاية من الاحتيال.	0.419	0.572
تقنية المعلومات تساعد في رصد ومعالجة الاحتيال بشكل فعال قبل حدوث الخسائر المالية.	0.617	0.455
تقنية المعلومات تعزز قدرة البنوك على الكشف المبكر عن محاولات الاحتيال والتدخل السريع لمنعها.	0.627	0.439
تقنية المعلومات تساعد في تقديم تحليلات دقيقة وموثوقة لتحديد وتقليل المخاطر المتعلقة بالاحتيال.	0.548	0.467
تقنية المعلومات تسهم في تطوير استراتيجيات متقدمة للوقاية من الاحتيال وتحسين استجابة البنوك لها.	0.595	0.487
المحور ككل	0,662	

لاحظ الباحث من الجدول رقم (6) أن قيم "ألفا كرونباخ" داخل الجدول أصغر من قيمة ألفا كرونباخ للمحور، وهذا يعني أن جميع العبارات داخل المحور متسقة مع بعضها البعض، كما أن معاملات الارتباط دالة معنويًا عند مستوى ٠,٠١ ويقصد بذلك العلاقة بين درجة العبارة والدرجة الكلية وهذا يعني صديق عبارات المقياس لهذا المحور.

المحور الثالث:

مدى تأثير تقنية المعلومات في الوقاية من الاحتيال بالبنوك التجارية السعودية

جدول رقم (7)

معاملات الاتساق والصدق لمحور مدى تأثير تقنية المعلومات في الوقاية من الاحتيال بالبنوك التجارية السعودية

عبارات المحور	ألفا كرونباخ *	معامل الارتباط **
تقنية المعلومات تساهم في تحقيق نتائج إيجابية في مكافحة الاحتيال بالبنوك التجارية السعودية.	0.797	0.561
تقنية المعلومات تعزز سمعة وثقة البنوك التجارية السعودية من خلال تحقيق أمان وسلامة المعاملات المالية.	0.804	0.516
تقنية المعلومات تحد من الخسائر المالية وتحسن الأداء المالي للبنوك التجارية السعودية.	0.787	0.615
تقنية المعلومات تساهم في تحسين بيئة الأعمال والتمويل في المملكة العربية السعودية.	0.776	0.671
تقنية المعلومات تلعب دوراً حيوياً في تحقيق استدامة النظام المالي والاقتصادي في المملكة العربية السعودية.	0.715	0.695
المحور ككل	0,820	

لاحظ الباحث من الجدول أن قيم ألفا كرونباخ داخل الجدول أصغر من قيمة "ألفا كرونباخ" للمحور، وهذا يعني أن جميع العبارات داخل المحور متسقة مع بعضها البعض، كما أن معاملات الارتباط دالة معنوياً عند مستوى ٠,٠١. ويقصد بذلك العلاقة بين درجة العبارة والدرجة الكلية وهذا يعني صدق عبارات المقياس لهذا المحور.

ثالثاً: الإحصاءات الوصفية للعبارات على شكل مقياس ليكرت (المعدل).

في هذا البند تم دراسة:

- توزيع مفردات العينة حسب فئات الآراء التي تم اختيارها، وبالتالي الحصول على عدد التكرارات في كل فئة والنسبة المئوية لهذه التكرارات.
- حساب المتوسط المرجح لهذه الآراء وحساب الانحراف المعياري لها.
- تحديد الرأي السائد للعينة وهو عبارة عن الفئة التي يقع فيها المتوسط المرجح.
- ترتيب أهمية العبارات.

قام الباحث بحساب المتوسط المرجح لإجابات عينة الدراسة على الأسئلة الواردة- في كل محور- على شكل يشابه لمقياس ليكرت الثنائي، واستخدام المتوسط المرجح إذا كان المتغير يأخذ قيمة تختلف من حيث أهميتها، لذلك يجب أخذ هذه الأهمية في الاعتبار وذلك بإعطاء كل إجابة الوزن المناسب لأهميتها، فتم إعطاء الأوزان التالية لفئات مقياس ليكرت الثنائي:

جدول رقم (8)

وزن الفئات

الوزن	الفئات
1	لا أوافق
2	أوافق

وذلك بهدف معرفة الفئة التي تنتمي إليها إجابات العينة، فحسب قيمة المتوسط المرجح لإجابات العينة تكون درجة المساهمة أو الرأي السائد للعينة كما يلي:

جدول رقم (9)

الرأي السائد للمتوسط المرجح

الرأي السائد	قيمة المتوسط المرجح
لا أوافق	من ١,٠٠ إلى أقل من ١,٥
أوافق	من ١,٥٠ إلى ٢,٠٠

الجزء الرابع

ملاحق الدراسة

لدراسة أهمية المحاور المختلفة تم تصنيف الإجابات في الجداول التالية وحساب درجة أهميتها وترتيبها حسب

هذه الأهمية.

ما درجة ممارسة عينة الدراسة للمحاور؟

المحور الأول: واقع فاعلية تقنية المعلومات في البنوك التجارية.

درجة ممارسة عينة الدراسة لعبارات محور "واقع فاعلية تقنية المعلومات في البنوك التجارية".

جدول رقم (10)

التوزيع التكراري والمتوسط المرجح والانحراف المعياري والرأي السائد لعبارات محور

"واقع فاعلية تقنية المعلومات في البنوك التجارية"

ترتيب الأهمية	الرأي السائد	الانحراف المعياري	المتوسط	أو وافق		لا أو وافق		العبارات
				%	التكرار	%	التكرار	
2	أوافق	0.47	1.67	68	38	32	12	تقنية المعلومات تساهم في تحسين أمان المعاملات في البنوك التجارية.
5	أوافق	0.50	1.52	70	35	30	15	البنوك التجارية تستخدم تقنية المعلومات بشكل فعال لتحليل البيانات المالية.
3	أوافق	0.47	1.66	74	37	26	13	تقنية المعلومات توفر وسائل فعّالة لتحقيق التواصل بين الفروع والمؤسسات المالية.
4	أوافق	0.48	1.66	68	34	32	16	تقنية المعلومات تعزز كفاءة إدارة العمليات والخدمات في البنوك التجارية.
1	أوافق	0.44	1.75	76	38	24	12	تقنية المعلومات تساهم في تطوير حلول متقدمة لمكافحة الاحتيال وضمان سلامة العمليات المالية.
	أوافق	0.48	1.65	0.65	182	0.35	68	الإجمالي لكل عبارات المحور

إن الرأي السائد لعبارات هذا المحور وللمحور ككل يقع في فئة "أوافق"، وهذا يعني أن عملاء المصارف

التجارية يوافقون على واقع فاعلية تقنية المعلومات في البنوك التجارية.

المحور الثاني: مدى مساهمة تقنية المعلومات في الوقاية من الاحتيال.

جدول رقم (11)

التوزيع التكراري والمتوسط المرجح والانحراف المعياري والرأي السائد لعبارات محور

"مدى مساهمة تقنية المعلومات في الوقاية من الاحتيال"

ترتيب الأهمية	الرأي السائد	الانحراف المعياري	المتوسط	أو وافق		لا أو وافق		العبارات
				%	التكرار	%	التكرار	
2	أوافق	0.45	1.71	72	36	28	14	تقنية المعلومات تسهم في تحديد الأنماط الغير معتادة في المعاملات المالية للوقاية من الاحتيال.
5	أوافق	0.31	1.89	90	45	10	5	تقنية المعلومات تساعد في رصد ومعالجة الاحتيال بشكل فعال قبل حدوث الخسائر المالية.
3	أوافق	0.46	1.69	68	32	32	16	تقنية المعلومات تعزز قدرة البنوك على الكشف المبكر عن محاولات الاحتيال والتدخل السريع لمنعها.
4	أوافق	0.48	1.55	60	30	40	20	تقنية المعلومات تساعد في تقديم تحليلات دقيقة وموثوقة لتحديد وتقليل المخاطر المتعلقة بالاحتيال.
1	أوافق	0.50	1.48	80	40	20	10	تقنية المعلومات تسهم في تطوير استراتيجيات متقدمة للوقاية من الاحتيال وتحسين استجابة البنوك لها.
	أوافق	0.42	1.76	0.76	113	0.24	35	الإجمالي لكل عبارات المحور

إن الرأي السائد لعبارات هذا المحور وللمحور ككل يقع في فئة "أوافق"، وهذا يعني أن عملاء المصارف

التجارية السعودية يوافقون على مدى مساهمة تقنية المعلومات في الوقاية من الاحتيال.

المحور الثالث: مدى تأثير تقنية المعلومات في الوقاية من الاحتيال بالبنوك التجارية السعودية.

جدول رقم (12)

التوزيع التكراري والمتوسط المرجح والانحراف المعياري والرأي السائد لعبارات محور

"مدى تأثير تقنية المعلومات في الوقاية من الاحتيال بالبنوك التجارية السعودية"

العبارات	لا أو افق		أو افق		المتوسط	الانحراف المعياري	الرأي السائد	ترتيب الأهمية
	التكرار	%	التكرار	%				
تقنية المعلومات تساهم في تحقيق نتائج إيجابية في مكافحة الاحتيال بالبنوك التجارية السعودية.	22	44	28	56	1.55	0.50	أو افق	3
تقنية المعلومات تعزز سمعة وثقة البنوك التجارية السعودية من خلال تحقيق أمان وسلامة المعاملات المالية.	12	24	38	76	1.76	0.43	أو افق	1
تقنية المعلومات تحد من الخسائر المالية وتحسن الأداء المالي للبنوك التجارية السعودية.	22	44	28	56	1.56	0.50	أو افق	4
تقنية المعلومات تساهم في تحسين بيئة الأعمال والتمويل في المملكة العربية السعودية.	27	54	23	46	1.46	0.50	لا أو افق	5
تقنية المعلومات تلعب دورًا حيويًا في تحقيق استدامة النظام المالي والاقتصادي في المملكة العربية السعودية.	35	70	15	30	1.16	0.52	أوافق	2
الإجمالي لكل عبارات المحور	83	0.38	117	0.62	1.62	0.49	أوافق	

إن الرأي السائد لمعظم عبارات هذا المحور وللمحور ككل يقع في فئة "أوافق"، وهذا يعني أن عملاء المصارف

التجارية السعودية يوافقون على مدى تأثير تقنية المعلومات في الوقاية من الاحتيال بالبنوك التجارية السعودية.

نتائج الدراسة:

على ضوء ما تقدم حيث يمكن عرض اهم النتائج التي توصلت اليها هذه الدراسة على النحو التالي أثبتت هذه الدراسة:

- أظهرت الدراسة أن تقنية المعلومات تساهم بشكل كبير في الوقاية من الاحتيال في البنوك التجارية، وذلك من خلال توفير أدوات متقدمة للكشف عن الاحتيال والتحقق من هوية المستخدمين ومراقبة الأنشطة المشبوهة.
- سلطت الدراسة الضوء على بعض الفجوات في تقنية المعلومات التي تجعل البنوك عرضة للهجمات الاحتيالية، مثل الضعف في إجراءات التحقق من الهوية أو قصور في نظام الرصد والكشف عن الأنشطة الغير معتادة.
- قدمت الدراسة توصيات عملية لتعزيز فعالية تقنية المعلومات في الوقاية من الاحتيال، مثل تحسين أدوات التحقق الثنائي، وتعزيز التدريب على الوعي الأمني، وتحسين أنظمة الرصد والتحليل.
- تمكنت الدراسة من تحليل تأثير استخدام تقنية المعلومات على الأداء العام للبنوك التجارية، بما في ذلك تأثيرها على الثقة بين العملاء والمستثمرين والمجتمع بشكل عام.

التوصيات

بناءً على النتائج التي تظهر من دراسة فعالية تقنية المعلومات في الوقاية من الاحتيال في البنوك التجارية السعودية، يمكن تقديم عدة توصيات للمؤسسات المالية والجهات المعنية بهذا الموضوع، وفيما يلي بعض التوصيات اللازمة:

1. تعزيز التدريب والتوعية الأمنية حيث ينبغي تعزيز برامج التدريب للموظفين والعملاء في البنوك التجارية لرفع مستوى الوعي بأهمية الأمن السيبراني ومخاطر الاحتيال، وتوفير توجيهات للتعرف على الاحتيال والتبليغ عنه.
 2. يجب تحسين أدوات التحقق الثنائي والتعرف البيومتري لزيادة مستوى الأمان في الوصول إلى الحسابات المصرفية والمعاملات المالية.
 3. ينبغي تطوير نظم الرصد والتحليل لزيادة قدرتها على اكتشاف الأنماط الغير معتادة والمشتبه بها في المعاملات المالية، واتخاذ إجراءات فورية للتحقق ومنع الاحتيال.
 4. ينبغي على البنوك التجارية تبني أحدث التقنيات والأدوات في مجال الذكاء الاصطناعي وتحليل البيانات الضخمة والتعلم الآلي لتعزيز قدراتها في مكافحة الاحتيال بشكل فعال.
 5. يجب تعزيز التعاون بين البنوك التجارية والجهات الحكومية والمنظمات الأخرى لتبادل المعلومات والخبرات في مكافحة الاحتيال، وتطوير إطار قانوني وتنظيمي مناسب لهذا الغرض.
 6. ينبغي تعزيز البنية التحتية السيبرانية للبنوك التجارية، بما في ذلك تحسين شبكات الاتصالات وتوفير جدران الحماية وتطبيق تقنيات التشفير لحماية البيانات المالية.
 7. يجب على البنوك والجهات الرقابية والتنظيمية تطوير وتعزيز السياسات والإجراءات الأمنية المتعلقة بالوقاية من الاحتيال، وضمان تطبيقها بشكل فعال.
- تلك التوصيات يمكن أن تساهم في تعزيز فعالية تقنية المعلومات في الوقاية من الاحتيال في البنوك التجارية وتقليل مخاطر الاحتيال المالي.

قائمة المراجع والمصادر

1. المدادحة، أحمد بن نافع. (2011). النشر الإلكتروني وحماية المعلومات، دار الصفاء للنشر والتوزيع، الأردن.
2. بكراري، نوال، شمعي لخضر. (2020). دور استخدام تكنولوجيا المعلومات في تقييم نظام المراقبة الداخلية – دراسة حالة بجامعة أدرار، مذكرة ضمن متطلبات نيل شهادة ماستر أكاديمي، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، الجزائر.
3. حبابية، مرفت. (2022). مكافحة الجريمة الإلكترونية دراسة مقارنة في التشريع الجزائري والفلسطيني، دار اليازوري للنشر والتوزيع. عمان. الأردن.
4. حسين، أسامه سمير. (2011). الاحتيال الإلكتروني، الأسباب والحلول، الطبعة الأولى، المنهل للنشر والتوزيع، بيروت. لبنان.
5. راشد، محمد المري. (2007). البث الأجنبي وتهديداته للأمن القومي، دار النهضة العربية، القاهرة.
6. علاء، عبد الرازق السلي. (2003). نظم إدارة المعلومات، المنظمة العربية للتنمية الإدارية، الدوحة، قطر.
7. عزة، فاروق عبد المعبود وطه محمد حسن. (2020). أمن المعلومات الرقمية وسبل حمايتها في ظل التشريعات الراهنة، المجلة المصرية لعلوم المعلومات، مج ٧، ع ١، بنى سويف، مصر.
8. عوف، الكفراوي. (2010). الرقابة المالية ما بين النظرية والتطبيق، مطبعة الأنصار، القاهرة.
9. غسان، قاسم اللامي. (2006). إدارة التكنولوجيا (مفاهيم ومداخل تقنيات تطبيقات علمية)، الطبعة الأولى، دار المناهج، عمان، الأردن.
10. فواز، سعد الدغيم. (2017). تأثير فعالية نظام الرقابة الداخلية على الحد من الغش والاحتيال في الشركات المساهمة العامة الكويتية، رسالة ماجستير، تخصص محاسبة، جامعة آل البيت.
11. محمد، إسماعيل. (2019). الأمن السيبراني في القطاع المصرفي، موجز سياسات، العدد الرابع، صندوق النقد العربي.
12. مؤسسة النقد العربي السعودي، إدارة التفتيش البنكي. (2008). دليل مكافحة الاختلاس والاحتيال المالي وإرشادات الرقابة. الإدارة العامة لمراقبة البنوك، الرياض.
13. حسين، محمد، الدويكات، الشبلي. (2009). سلسلة الجرائم المالية والمستحدثة، التزوير والاحتيال بالبطاقات الائتمانية، المنهل للطباعة والنشر، بيروت، لبنان.

14. شمس الدين، فيصل هاشم. (2008). تقنية المعلومات، المصطلحات، وسائل الاتصال، التوظيف، الثقافة، الطبعة الأولى، الناشر: شمس للنشر والتوزيع، القاهرة.
15. عقيل، محمد عقيل. (2014). أساسيات تقنية المعلومات. المنهل للطباعة والنشر. بيروت. لبنان.
16. العوجي، فريج سعيد. (2016). حروب تقنية المعلومات. الطبعة الأولى. دار العلوم العربية للنشر والتوزيع. القاهرة.
17. عمر، محمد حسن. (1997). الإدارة والتقنية ، شركاء في مواجهة تحديات عصر الانترنت، مؤسسة الفلاح للترجمة والنشر والتوزيع، القاهرة.
18. إبراهيم، راشد بشير. (2008). التحقيق الجنائي في جرائم تقنية المعلومات، الطبعة الأولى. مركز الإمارات للدراسات والبحوث الاستراتيجية، العدد 131. أبوظبي.
19. فكري، أيمن عبدالله. (2014). الجرائم المعلوماتية. دراسة مقارنة في التشريعات العربية والأجنبية. الطبعة الأولى. مكتبة القانون والاقتصاد. الرياض.

الملاحق

الملحق (1)

جامعة الجميع الذكية

كلية الإدارة

مشروع التخرج

المكرم/ أخي العميل - حفظه الله -

سلام الله عليكم ورحمته وبركاته، أما بعد،،،

أرجو العمل على تعبئة هذه الاستبانة، والتي تحتاج إلى درجة عالية من المسؤولية والتركيز.

علماً بأن تعبئة هذه الاستبانة يأتي ضمن إجراءات دراسة علمية بعنوان:

" فاعلية تقنية المعلومات في الوقاية من الاحتيال بالبنوك التجارية السعودية "

الدراسة هي ضمن متطلبات الحصول على درجة الماجستير في الإدارة، أمل منكم استيفاء تعبئة الاستبانة

بوضع علامة (√) أمام الإجابة المناسبة.

إن جميع البيانات الواردة في الاستبيان سرية للغاية ولن تستخدم إلا لأغراض البحث العلمي.

شاكراً لكم تعاونكم

وتفضلوا بقبول فائق الاحترام،،،

الباحث

القسم الاول: الخصائص الديموغرافية:

يرجي الإجابة عن الأسئلة الآتية التي تتضمن معلومات عامة تتعلق بالمستجيب، من خلال وضع إشارة (√) في المكان المناسب.

1. العمر:

☐ من 20 سنة إلى 25 سنة.

☐ من 25 سنة إلى 30 سنة.

☐ من 30 سنة إلى 35 سنة.

☐ أكثر من 35 سنة.

2. المؤهل العلمي:

☐ الثانوية العامة فما دون.

☐ دبلوم.

☐ بكالوريوس.

☐ ماجستير فأعلى.

3. عدد سنوات التعامل مع المصارف التجارية:

☐ من سنة - أقل من خمس سنوات.

☐ من خمس سنوات - أقل من عشر سنوات.

☐ من عشر سنوات إلى أقل من 15 سنة.

☐ من 15 سنة فأكثر.

القسم الثاني:

فيما يأتي مجموعة من العبارات الخاصة لفاعلية تقنية المعلومات في الوقاية من الاحتيال بالبنوك التجارية السعودية، يرجى

التكرم باختيار الاجابة المناسبة بعد قراءة العبارات الآتية:

■ المعيار الأول: واقع فاعلية تقنية المعلومات في البنوك التجارية.

م	عبارات المحور	موافق بشدة	موافق	لاوافق	لاوافق بشدة
1	تقنية المعلومات تساهم في تحسين أمان المعاملات في البنوك التجارية.				
2	البنوك التجارية تستخدم تقنية المعلومات بشكل فعال لتحليل البيانات المالية.				
3	تقنية المعلومات توفر وسائل فعالة لتحقيق التواصل بين الفروع والمؤسسات المالية.				
4	تقنية المعلومات تعزز كفاءة إدارة العمليات والخدمات في البنوك التجارية.				
5	تقنية المعلومات تساهم في تطوير حلول متقدمة لمكافحة الاحتيال وضمان سلامة العمليات المالية.				

■ المعيار الثاني: مدى مساهمة تقنية المعلومات في الوقاية من الاحتيال.

م	عبارات المحور	موافق بشدة	موافق	لاوافق	لاوافق بشدة
1	تقنية المعلومات تساهم في تحديد الأنماط الغير معتادة في المعاملات المالية للوقاية من الاحتيال.				
2	تقنية المعلومات تساعد في رصد ومعالجة الاحتيال بشكل فعال قبل حدوث الخسائر المالية.				
3	تقنية المعلومات تعزز قدرة البنوك على الكشف المبكر عن محاولات الاحتيال والتدخل السريع لمنعها.				
4	تقنية المعلومات تساعد في تقديم تحليلات دقيقة وموثوقة لتحديد وتقليل المخاطر المتعلقة بالاحتيال.				
5	تقنية المعلومات تساهم في تطوير استراتيجيات متقدمة للوقاية من الاحتيال وتحسين استجابة البنوك لها.				

■ المعيار الثالث: مدى تأثير تقنية المعلومات في الوقاية من الاحتيال بالبنوك التجارية السعودية

م	عبارات المحور	موافق بشدة	موافق	لاوافق	لاوافق بشدة
1	تقنية المعلومات تساهم في تحقيق نتائج إيجابية في مكافحة الاحتيال بالبنوك التجارية السعودية.				
2	تقنية المعلومات تعزز سمعة وثقة البنوك التجارية السعودية من خلال تحقيق أمان وسلامة المعاملات المالية.				
3	تقنية المعلومات تحد من الخسائر المالية وتحسن الأداء المالي للبنوك التجارية السعودية.				
4	تقنية المعلومات تساهم في تحسين بيئة الأعمال والتمويل في المملكة العربية السعودية.				
5	تقنية المعلومات تلعب دورًا حيويًا في تحقيق استدامة النظام المالي والاقتصادي في المملكة العربية السعودية.				