



يوم: 2026/01/13

امتحان الدورة العادية في مقياس التكنولوجيا المالية

السؤال الأول: أجب بصحيح أو خطأ مع تصحيح الخطأ إن وجد

- 1- تعتبر البيانات المستمدة من وسائل التواصل الاجتماعي (Facebook, X) بيانات "مهيكلية" (Structured Data) "
- 2- خاصية "السرعة" (Velocity) "في البيانات الضخمة تعني فقط سرعة نقل البيانات عبر الإنترنت
- 3- تعتبر بيانات إنترنت الأشياء (IoT) من المصادر التقليدية للبيانات في المصارف المركزية.
- 4- نموذج "التأمين الأصغر" (Micro-Insurance) "مصمم خصيصاً لحماية أصحاب الدخل المرتفع ضد مخاطر ضخمة.
- 5- تهدف الخدمات المصرفية المفتوحة (Open Banking) إلى تقليل المنافسة في السوق المالي.
- 6- في التمويل الجماعي القائم على "المكافآت" (Rewards) "، يحصل الممول على نسبة من أرباح الشركة السنوية
- 7- تعتمد "التغطية المرنة" (Flexible Coverage) "في التأمين على دفع أقساط ثابتة سنوياً بغض النظر عن استخدام العميل
- 8- التأمين من الند للند (P2P Insurance) "هو نموذج يعتمد على تجمع مجموعة من الأفراد لتأمين بعضهم البعض وتشارك المخاطر
- 9- يساهم استخدام أجهزة الاستشعار (Telematics) في السيارات في تحديد قسط التأمين بناءً على سلوك القيادة الفعلي للسائق.
- 10- تعتمد الخدمات المصرفية المفتوحة بشكل أساسي على "واجهات برمجة التطبيقات" (APIs) "لمشاركة البيانات.
- 11- تؤدي الخدمات المصرفية المفتوحة إلى زيادة احتكار البنوك الكبرى للبيانات المالية للعملاء
- 12- التحليلات التنبؤية تهدف إلى استخدام البيانات التاريخية لتوقع الأحداث المستقبلية.

السؤال الثاني: أجب على الأسئلة التالية باختصار

- 1- حدد العلاقة بين "الخدمات المصرفية المفتوحة" (Open Banking) و"واجهات برمجة التطبيقات" (APIs) "
- 2- حدد الفرق بين التعلم الآلي/ التعلم العميق

السؤال الثالث: ماهي التقنيات المناسبة للجمل التالية

- الكشف عن عمليات الاحتيال وغسل الأموال في الوقت الفعلي
- توقع العملاء الذين قد يتركوا البنك
- التقنيات التي تسمح بمشاركة البيانات المالية للعملاء بين البنوك وشركات الطرف الثالث
- أصول معلوماتية كبيرة الحجم وسريعة التدفق تتطلب طرق معالجة مبتكرة.
- استخدام التكنولوجيا والابتكارات الرقمية في قطاع التأمين لخلق نماذج أعمال جديدة

السؤال الرابع: أجب على الأسئلة التالية باختصار

- 1- تعد المنصات الرقمية (Digital Platforms) حجر الزاوية في التحول المالي الحديث، حيث تعمل كوسيط تكنولوجي يربط بين مختلف الأطراف. حدد دور هذه المنصات في كسر احتكار المؤسسات المالية التقليدية، موضحاً كيف تساهم في تعزيز الشمول المالي ؟
- 2- تعتبر مخاطر الأمن السيبراني (Cybersecurity Risks) التهديد الأكثر خطورة في بيئة التكنولوجيا المالية، بالإضافة إلى مخاطر الاحتيال المالي ومخاطر البيانات والخصوصية. ومع ذلك فإن الرقابة لا تهدف فقط إلى منع الاختراقات بل إلى موازنة الابتكار مع الاستقرار المالي. اشرح هذه المخاطر، وما هي أدوات الرقابة الأنسب لإدارتها.

**ملاحظة هامة. تنظم الإجابة على جميع الأسئلة في جدول



الإجابة النموذجية لامتحان الدورة العادية في مقياس التكنولوجيا المالية

العلامة	السؤال الأول
0.5	1- تعتبر البيانات المستمدة من وسائل التواصل الاجتماعي (Facebook, X) بيانات "مهيكلية" (Structured Data). خطأ، هي بيانات غير مهيكلية [Unstructured]
0.5	2- خاصية "السرعة" (Velocity) في البيانات الضخمة تعني فقط سرعة نقل البيانات عبر الإنترنت. خطأ، تعني سرعة توليد البيانات وتدفقها والحاجة لمعالجتها في الوقت الفعلي]
0.5	3- تعتبر بيانات إنترنت الأشياء (IoT) من المصادر التقليدية للبيانات في المصارف المركزية. خطأ، تعتبر من المصادر البديلة الحديثة.
0.5	4- نموذج "التأمين الأصغر" (Micro-Insurance) مصمم خصيصاً لحماية أصحاب الدخل المرتفع ضد مخاطر ضخمة. خطأ، مصمم لحماية أصحاب الدخل المنخفض ضد مخاطر محددة، مصادر: 538 (من سياق النماذج)
0.5	5- التمويل القائم على "الأشهر" يمنح الممولين حصص ملكية في الشركات الناشئة مقابل مساهماتهم. صحيح
0.5	6- في التمويل الجماعي القائم على "المكافآت" (Rewards)، يحصل الممول على نسبة من أرباح الشركة السنوية. خطأ، يحصل على منتج أو خدمة أو هدية رمزية وليس أرباحاً مالية]
0.5	7- تعتمد "التغطية المرنة" (Flexible Coverage) في التأمين على دفع أقساط ثابتة سنوياً بغض النظر عن استخدام العميل. خطأ، تعتمد على تفعيل أو إيقاف التغطية حسب الحاجة أو الاستخدام الفعلي]
0.5	8- التأمين من الند للند (P2P Insurance) هو نموذج يعتمد على تجمع مجموعة من الأفراد لتأمين بعضهم البعض وتشارك المخاطر. صحيح]
0.5	9- يساهم استخدام أجهزة الاستشعار (Telematics) في السيارات في تحديد قسط التأمين بناءً على سلوك القيادة الفعلي للسائق. صحيح]
0.5	10- تعتمد الخدمات المصرفية المفتوحة بشكل أساسي على "واجهات برمجة التطبيقات" (APIs) لمشاركة البيانات. صحيح
0.5	11- تؤدي الخدمات المصرفية المفتوحة إلى زيادة احتكار البنوك الكبرى للبيانات المالية للعملاء. خطأ، تهدف لتمكين العميل من مشاركة بياناته مع مزودين آخرين لزيادة المنافسة
0.5	12- التحليلات التنبؤية تهدف إلى استخدام البيانات التاريخية لتوقع الأحداث المستقبلية. صحيح،
06.00	الملاحظة: لا يتحصل الطالب على علامة (0.5) إلا إذا كانت تحليل الإجابة صحيح
	المجموع السؤال الأول
النقاط	السؤال الثاني

<p>01</p> <p>0.5</p> <p>0.5</p>	<p>1- حدد العلاقة بين "الخدمات المصرفية المفتوحة (Open Banking)" و"واجهات برمجة التطبيقات (APIs)"</p> <p>حلل العلاقة بين "الخدمات المصرفية المفتوحة (Open Banking)" و"واجهات برمجة التطبيقات (APIs)"</p> <ul style="list-style-type: none"> تعتمد الخدمات المصرفية المفتوحة كلياً على الـ APIs كأداة تقنية تسمح بمشاركة بيانات العملاء بين البنوك ومزودي الطرف الثالث بأمان، مما يخلق منافسة ويسمح بتقديم خدمات مخصصة <p>2- حدد الفرق بين التعلم الآلي/ التعلم العميق</p> <p>التعلم الآلي: أحد خواص الذكاء الاصطناعي في تحليل البيانات المالية، وتكمن ماهية هذه التقنية في قدرة الذكاء الاصطناعي على بناء نماذج وخوارزميات تستخدم البيانات السابقة التي زُوِّدت بها، في التدريب والتعلم عوضاً عن تزويدها بالقواعد التفصيلية لكل حالة. فهي تستمد القواعد وتستخلصها من خلال البيانات التاريخية مثل (المعاملات المالية، والتقارير، وأسعار الأسهم). بعد التدريب والتعلم يستطيع AI الكشف عن العلاقات والأنماط داخل البيانات ثم يطرح تنبؤاً خاصاً بالمستقبل.</p> <p>التعلم العميق: محاولة الذكاء الاصطناعي لمحاكاة طريقة عمل الدماغ البشري؛ وهي قفزة نوعية في عالم تحليل البيانات. يرتبط بشكل مباشر بالتعلم الآلي ويُعد فرعاً منه، ينمو إلى مستوى أعلى من مجرد القدرة على التعلم والتدريب، فهو يتخطى ذلك إلى بناء شبكات عصبية اصطناعية Artificial Neural Networks ذات طبقات عدة.</p>
<p>02</p>	<p>المجموع السؤال الثاني</p>
<p>النقاط</p>	<p>السؤال الثالث</p>
<p>0.5 نقطة</p> <p>2.5</p>	<p>-الكشف عن عمليات الاحتيال وغسل الأموال في الوقت الفعلي الذكاء الاصطناعي</p> <p>- توقع العملاء الذين قد يتركوا البنك التحليلات التنبؤية</p> <p>- التقنيات التي تسمح بمشاركة البيانات المالية للعملاء بين البنوك وشركات الطرف الثالث المصرفية المفتوحة أو أواجهات برمجة التطبيقات (APIs)</p> <p>- أصول معلوماتية كبيرة الحجم وسريعة التدفق تتطلب طرق معالجة مبتكرة. البيانات الضخمة</p> <p>- استخدام التكنولوجيا 1 والابتكارات الرقمية في قطاع التأمين لخلق نماذج أعمال جديدة. تكنولوجيا التأمين</p> <p>المجموع</p>
	<p>السؤال الرابع</p> <p>"تُعد المنصات الرقمية (Digital Platforms) حجر الزاوية في التحول المالي الحديث، حيث تعمل كوسيط تكنولوجي يربط بين مختلف الأطراف. ناقش دور هذه المنصات في كسر احتكار المؤسسات المالية التقليدية، موضحاً كيف تساهم في تعزيز 'الشمول المالي'."</p> <p>الإجابة النموذجية (التحليل):</p>

<p>02</p>	<p>- دور المنصات في كسر الاحتكار:</p> <ul style="list-style-type: none"> تعمل المنصات الرقمية على تقليل "حواجز الدخول" (Barriers to Entry) "أمام اللاعبين الجدد. فبينما كانت الخدمات المالية حكراً على البنوك الضخمة ذات الفروع المادية. سمحت المنصات لشركات ناشئة بتقديم خدمات (إقراض، تأمين، استثمار) بتكاليف تشغيلية منخفضة جداً. من خلال واجهات برمجة التطبيقات (APIs) في الخدمات المصرفية المفتوحة، لم تعد البيانات ملكاً حصرياً للبنك، بل أصبح بإمكان المنصات الرقمية الوصول إليها (بإذن العميل) لتقديم بدائل مالية أكثر تنافسية وأقل سعراً. <p>- تعزيز الشمول المالي (أمثلة تطبيقية):</p> <ul style="list-style-type: none"> في التمويل الجماعي (Crowdfunding) نجحت المنصات في توفير بديل تمويلي للمشاريع الصغيرة والمتوسطة والشركات الناشئة التي غالباً ما يرفضها القطاع البنكي التقليدي لعدم وجود ضمانات. المنصة هنا تجمع مبالغ صغيرة من جمهور واسع، مما يفتح باب التمويل لفئات كانت "مستبعدة مالياً". في تكنولوجيا التأمين (InsurTech) من خلال منصات "التأمين الأصغر" (Micro-Insurance)، يتم استهداف ذوي الدخل المنخفض بوثائق تأمين بسيطة ومرنة وبأقساط زهيدة تتناسب مع قدرتهم الشرائية، وهو ما لا توفره شركات التأمين التقليدية الكبرى.
<p>01.5</p>	<p>هي أخطر أنواع المخاطر في FinTech. تعتبر مخاطر الأمن السيبراني (Cybersecurity Risks) التهديد الأكثر خطورة في بيئة التكنولوجيا المالية، بالإضافة إلى مخاطر الاحتيال المالي ومخاطر البيانات والخصوصية. ومع ذلك فإن الرقابة لا تهدف فقط إلى منع الاختراقات بل إلى موازنة الابتكار مع الاستقرار المالي. اشرح هذه المخاطر، وما هي أدوات الرقابة الأنسب لإدارتها.</p> <p>1- مخاطر الأمن السيبراني</p> <p>تشمل:</p> <p>الاختراقات: دخول غير مصرح إلى أنظمة البنوك أو المحافظ.</p> <p>البرمجيات الخبيثة: فيروسات</p> <p>هجمات الفدية: تشفير البيانات والمطالبة بمبلغ مالي لفكها.</p> <p>التصيد: إرسال رسائل مزيفة لسرقة بيانات العملاء.</p> <p>مثال: اختراق بيانات بطاقات الدفع لموقع تجاري بسبب ضعف التشفير</p> <p>2- مخاطر الاحتيال المالي</p> <p>تحدث عندما يحاول المجرمون استغلال الأنظمة المالية لتحقيق مكاسب غير مشروعة.</p> <p>صور الاحتيال:</p> <p>سرقة حسابات المحافظ الإلكترونية</p> <p>استعمال بطاقات مسروقة</p> <p>التلاعب في المعاملات</p> <p>إنشاء طلبات تحويل وهمية</p> <p>مزيفة تدعو المستخدم لتحديث بياناته البنكية ثم يتم الاستيلاء على حسابه. SMS مثال: رسالة</p> <p>3- مخاطر البيانات والخصوصية</p> <p>التكنولوجيا المالية تعتمد على جمع كمية كبيرة من البيانات: بيانات شخصية</p>

01.5	بيانات مالية سلوك المستخدم أي خلل في حماية هذه البيانات يؤدي إلى تسريبها أو استخدامها دون إذن مثال: تسريب بيانات 100 ألف مستخدم من تطبيق محفظة إلكترونية بسبب خلل في الخوادم أدوات الرقابة 1. التشريعات والقوانين 2. التعليمات التنظيمية 3. التنظيمي SandBox 4. شروط الترخيص
20	المجموع الكلي