

الإرشادات والمعايير الإضافية لطلب منح الترخيص للبنوك الرقمية في المملكة العربية السعودية

فبراير ٢٠٢٠ م

المحتويات

الصفحة

٣	مقدمة
٣	الغرض ونطاق التطبيق
٣	الشروط الواجب توافرها في طلب الترخيص
٣	خطة العمل
٣	متطلبات رأس المال والسيولة
٤	التواجد المكاني
٤	الحوكمة
٤	إدارة المخاطر والرقابة
٤	الالتزام ومكافحة غسل الأموال وتمويل الإرهاب
٤	مخاطر التقنية والأمن السيبراني
٤	التقييم المستقل
٥	إسناد المهام إلى طرف ثالث
٥	خطة الخروج
٥	المتطلبات الاحترافية والإشرافية
٥	حماية العملاء

مقدمة

استناداً إلى الصلاحيات الممنوحة لمؤسسة النقد العربي السعودي بموجب أحكام نظامها الصادر بالمرسوم الملكي رقم (٢٣) وتاريخ ١٣٧٧/٥/٢٣ هـ، وأحكام نظام مراقبة البنوك، الصادر بالمرسوم الملكي رقم (٥/م) وتاريخ ١٣٨٦/٢/٢٢ هـ، أُصدرت هذه الإرشادات والمعايير الإضافية لطلبات منح التراخيص لإنشاء بنوك رقمية في المملكة العربية السعودية.

الغرض ونطاق التطبيق

- ١- تهدف هذه الإرشادات إلى تحديد معايير الترخيص لإنشاء البنوك الرقمية، والتي يقصد بها -لغرض تطبيق أحكام هذه الإرشادات-؛ البنوك التي تزاوّل الأعمال المصرفية بشكلٍ أساسي عن طريق القنوات الرقمية كشبكة الانترنت وتطبيقات الجوال.
- ٢- تسري هذه الإرشادات على طلبات الحصول على تراخيص لإنشاء البنوك الرقمية في المملكة، ويتعين الالتزام بهذه الإرشادات كمتطلبات إضافية لما جاء في الإرشادات والمعايير الأساسية لطلب منح الترخيص لمزاولة الأعمال المصرفية المنشورة على موقع المؤسسة الإلكتروني.

الشروط الواجب توافرها في طلب الترخيص

يشترط لتقديم طلب ترخيص بنك رقمي في المملكة استيفاء الآتي:

- ١- أن يتخذ البنك الرقمي شكل شركة مساهمة محلية.
- ٢- أن يتوافر لدى المؤسسين ما يلي:
 - أ- خبرة ومعرفة في مجال القطاع المالي.
 - ب- خبرة ومعرفة مناسبة ذات صلة بالتقنية.
 - ج- الأهلية والقدرة والملاءة المالية لدعم تأسيس البنك الرقمي.
- ٣- يجب أن يكون لدى المتقدمين فريق من الأفراد من ذوي الخبرات في مجالاتهم وذلك لمناقشة الجوانب ذات العلاقة بالطلب المقدم.

خطة العمل

يتعين في طلب الترخيص إرفاق خطة عمل واضحة تغطي بحد أدنى ما يلي:

- ١) خطة البنية التحتية لتقنية المعلومات والتقنيات المبتكرة التي سيتم طرحها.
- ٢) التوقعات المالية.
- ٣) الفئة المستهدفة شاملة الدراسة والتحليل الأساسي.
- ٤) المنتجات والخدمات المقترحة بما يتفق مع الفئات المستهدفة.

متطلبات رأس المال والسيولة

على المتقدمين تقديم خطة التقييم الداخلي لكفاية رأس المال وخطة التقييم الداخلي لكفاية السيولة مع طلب الترخيص للبنك. وسوف تقوم المؤسسة بإجراء تقييم مدى كفاية رأس المال لمقدم الطلب وفقاً لكل حالة على حده، استناداً إلى حجم العمليات

وطبيعتها ودرجة تعقيدها حسب ما هو مقترح في خطة العمل، وخطة التقييم الداخلي لكفاية رأس المال وخطة التقييم الداخلي لكفاية السيولة.

التواجد المكاني

على طالبي الترخيص لإنشاء بنك رقمي إيجاد وتخصيص مقر لمزاولة البنك الرقمي عمله، ويكون هذا المقر المركز الرئيس له، على أنه ليس متطلباً أن تقوم البنوك الرقمية بفتح فروع لها، وذلك مع مراعاة بعض الحالات الاستثنائية التي قد تشترط المؤسسة على البنك الرقمي تأسيس مراكز لتسهيل الوصول للعملاء للتعامل مع الاستفسارات والشكاوى.

الحوكمة

يجب على البنوك الرقمية اتباع المبادئ الرئيسة للحوكمة في البنوك العاملة بالمملكة العربية السعودية والصادرة عن المؤسسة، كما هو مطبق مع البنوك التقليدية.

إدارة المخاطر والرقابة

يجب على البنوك الرقمية أن تثبت للمؤسسة بأن سياساتها المقترحة لإدارة المخاطر والرقابة كافية ومناسبة لرصد مخاطر التعرض أو الانكشاف والحد منها، وذلك وفقاً للفقرة (د) من الإرشادات والمعايير الأساسية لطلب منح الترخيص لمزاولة الأعمال المصرفية في المملكة.

الالتزام ومكافحة غسل الأموال وتمويل الإرهاب

يتعين أن يرفق في طلب الترخيص الضوابط المحددة لمكافحة غسل الأموال وتمويل الإرهاب بما يتفق مع الخدمات الرقمية المستهدف تقديمها، بالإضافة إلى إثبات الالتزام بالمتطلبات الواردة في الفقرة (هـ) من الإرشادات والمعايير الأساسية لطلب منح الترخيص لمزاولة الأعمال المصرفية الصادرة عن المؤسسة.

مخاطر التقنية والأمن السيبراني

- 1- على طالبي الترخيص الأخذ بعين الاعتبار أن أمن المعلومات ومتانة النظم وتوفرها من المكونات الرئيسة للبنك الرقمي، ويجب أن يتناسب اختيار التقنيات والترتيبات الأمنية مع المنتجات والخدمات المصرفية المستهدف تقديمها.
- 2- يتعين أن يُرفق في طلب الترخيص ما يُثبت توافق تصميم وتطبيق التقنية وإطار الأمن السيبراني مع جميع المتطلبات ذات الصلة الصادرة عن المؤسسة أو غيرها من الجهات ذات العلاقة، ومن ذلك على سبيل المثال لا الحصر، إطار عمل الأمن السيبراني، وإطار إدارة استمرارية الأعمال الصادرين عن المؤسسة. والتعليمات الصادرة عن الهيئة الوطنية للأمن السيبراني.

التقييم المستقل

للمؤسسة أن تشترط على طالبي الترخيص تعيين جهة تقييم مؤهلة وذات خبرة "المقيّم" لإجراء تقييم لمجالات فنية محددة على نفقة طالب الترخيص، ومنها على سبيل المثال: التقنية والأمن السيبراني وترتيبات مكافحة غسل الأموال وتمويل الإرهاب، حسب الآتي:

- 1- مرحلة التصميم- بعد تقديم الطلب إلى المؤسسة، يتعين على جهة التقييم إجراء تقييم مدى كفاءة الحوكمة والعمليات والأنظمة المقترحة للتصميم المقترح وفق طلب الترخيص. وستطلب المؤسسة من المتقدم تزويدها بتقرير تقييم مرحلة

التصميم المقترح مرفق به خطة لمعالجة الملاحظات/التحفظات (إن وجدت)، وعلى المتقدم معالجة الملاحظات/التحفظات الرئيسة بالشكل المناسب.

٢- مرحلة التنفيذ- يجب على جهة التقييم إجراء تقييم مفصل قبل بدء العمليات حول تنفيذ الفقرة (أ) أعلاه، وسوف تطلب المؤسسة من المتقدم تزويدها بتقرير تقييم مرحلة التنفيذ وفقاً للتصميم المعتمد بالإضافة إلى خطة معالجة الملاحظات/التحفظات (إن وجدت)، وعلى المتقدم معالجة الملاحظات/التحفظات الرئيسة بالشكل المناسب للحصول على موافقة المؤسسة على الإطلاق الرسمي.

إسناد المهام إلى طرف ثالث

يجب أن تحقق عمليات الإسناد الخارجي المتوقعة للعمليات والموظفين والأنظمة الجوهرية متطلبات الإسناد الواردة في تعليمات إسناد مهام لطرف ثالث الصادرة عن المؤسسة.

خطة الخروج

- ١- يتعين على المتقدمين تقديم خطة خروج في حال واجهوا صعوبات في تحقيق أهداف العمل المنشودة.
- ٢- يجب أن تكون خطة الخروج واضحة وتبين الخطوات التي سيتم اتخاذها لإدارة أموال العملاء والأعمال القائمة، على سبيل المثال؛ قد يتضمن ذلك ترحيل الحسابات المصرفية والأموال المرتبطة بها إلى بنك آخر، وضمان استمرار الخدمات للعملاء الحاليين وإدارة الأصول والخصوم الأخرى، وغيرها.

المتطلبات الاحترازية والإشرافية

- ١- تخضع البنوك الرقمية للمتطلبات الاحترازية ذاتها التي تخضع لها باقي البنوك.
- ٢- نظراً لطبيعة عمل البنك؛ يتوقع أن تكون البيانات الإشرافية (أو الغالب منها) بصيغة إلكترونية، ويتعين أن تتميز الحلول التقنية لدى البنك الرقمي بالوصول السهل والسريع إلى المعلومات بشكل دقيق وكامل لتمكين المؤسسة من أداء مهامها الإشرافية والرقابية.

حماية العملاء

- ١- تنطبق مبادئ حماية عملاء المصارف الصادرة عن المؤسسة على البنوك الرقمية أيضاً.
- ٢- يتعين أن يُرفق في طلب الترخيص ما يُثبت وجود الترتيبات والقنوات الضرورية لحماية ودعم العملاء بشكل كافٍ خلال جميع مراحل الخدمات المصرفية.
