الرقم: 115/م ن
التاريخ: 2022/5/23

مجلس النقد والتسليف، بناء على أحكام قانون مصرف سورية المركزي ونظام النقد الأساسي رقم /23/ لعام 2002 وتعديلاته، وعلى كتاب مديرية مفوضية الحكومة لدى المصارف رقم 16/1268/ص تاريخ 2022/3/10، وعلى مذاكرته في جلسته المنعقدة بتاريخ 2022/5/19، يقرر ما يلي:

أولاً: الموافقة على الإطار المعياري لمهام التدقيق المعلوماتي الخارجي لدى المصارف والمؤسسات المالية العاملة في الجمهورية العربية السورية والمبين فيما يلي:

المادة 1- التعاريف:

- المؤسسة: المؤسسة المالية المصرفية
- المدقق المعلوماتي الخارجي: شخص اعتباري/ شركة سورية مسجلة في سجل الشركات في وزارة التجارة الداخلية وحماية المستهلك وفقاً للتشريعات والقوانين النافذة، وحاصلة على اعتمادية من الهيئة الوطنية لخدمات الشبكة في تقديم خدمات أمن المعلومات.
- البيانات الحساسة: كافة بيانات ومعلومات النظم والتقنيات المستثمرة في المؤسسة وكافة بيانات العملاء والعمليات وبكافة تفاصيلها بشكلها الالكتروني ووسائط حفظها وتخزينها.
- التدقيق المعلوماتي: مراجعة وتقييم الضوابط الإدارية والقانونية والاستثمارية والتشغيلية لنظم تقانة المعلومات والبنى التقنية المستثمرة في المؤسسة وكافة العمليات المنفذة عليها وكافة السياسات والإجراءات المتعلقة بها، وبيان الرأي والنتائج بناءً على تحليل للمخاطر المرتبطة وفقاً للمعايير والضوابط ذات الصلة المعتمدة من مجلس النقد والتسليف ومصرف سورية المركزي بمدى تحقيق المؤسسة للأهداف المحددة في البند 3.2 من هذا القرار.

المادة 2- تلتزم المؤسسة بالتعاقد مع مدقق خارجي لتدقيق نظم المعلومات بغرض تحقيق الأهداف التالية:

2.1. التأكد من سرية المعلومات والبيانات الحساسة وأمنها وحمايتها من الإفصاح غير المصرح به نتيجة لعوامل داخلية وخارجية.

2.2. التأكد من سلامة البيانات ودقة وكفاية وكفاءة وفعالية المعلومات وصلاحيتها وموثوقيتها واعتماديتها في اتخاذ القرارات.

2.3. التأكد من توافر المعلومات وتكاملیتها وشموليتها عند طلبها وحماية الموارد المرتبطة بها ومدى استمرارية العمل والاستعادة عند الاقتضاء.

2.4. التأكد من موثوقية البنى التقنية ونظم المعلومات واستقلاليتها ومدى قدرتها على تنفيذ كافة أنواع الوظائف والعمليات الاستثمارية في مختلف الظروف التشغيلية، ومدى كفاية متطلبات استمراريتها واستقلاليتها.

2.5. تقييم الامتثال للضوابط واللوائح والتعاميم والالتزامات القانونية والتنظيمية المعتمدة من مجلس النقد والتسليف ومصرف سورية المركزي والمعايير الوطنية والعالمية.

المادة 3-الإجراءات التنظيمية والإدارية لعملية التدقيق المعلوماتي:

3.1. أن يكون لدى المدقق المعلوماتي الخارجي خبرات وممارسة فعلية في مجال التدقيق مع فريق عمل متخصص وذو خبرة وتجارب سابقة وسمعة جيدة في هذا المجال، إضافة إلى عنوان دائم في سورية، مع مراعاة أصول التعاقد المعتمدة لدى المؤسسة.

3.2. أن يكون القانون السوري هو القانون الواجب التطبيق في العلاقة بين المؤسسة والمدقق الخارجي.

3.3. أن تكون الشركة حاصلة على اعتمادية سارية المفعول من الهيئة الوطنية لخدمات الشبكة وفق الضوابط المعمول بها بهذا الخصوص في تقديم خدمات أمن المعلومات.

3.4. توقيع المدقق المعلوماتي الخارجي على اتفاقية عدم إفصاح والحفاظ على السرية موثقة برقم وتاريخ أصولاً قبل البدء بأية مناقشات أو مفاوضات حول المهمة مع المؤسسة.

3.5. الطلب إلى المدقق المعلوماتي الخارجي تزويد المؤسسة بالمعلومات الآتية (*بالحد الأدنى*):

3.5.1. نسخة عن الهيكلية الإدارية للمدقق مع مسمياتها الوظيفية.

3.5.2. تحديد كافة الأطراف التي سوف يكون لها دور واطلاع في سياق تنفيذ مهمة التدقيق المعلوماتي ونشاطاتها ونتائجها وتقاريرها.

3.5.3. تحديد آلية للتحكم بكافة الجوانب المتعلقة بالحصول على البيانات والمعلومات وحفظها والتصريح عنها.

3.5.4. إثبات للخبرة مع وثائق مؤيدة مصدقة أصولاً.

3.6. يتم توثيق كافة المستندات والمراسلات المتعلقة بالمدقق المعلوماتي الخارجي التي تمت قبل توقيع العقد معه في مقدمة ذلك العقد؛ وتوثيق العقد برقم وتاريخ مرجعي.

3.7. تقييم كفاءة المدقق الخارجي واختياره استناداً للحد الأدنى من الأسس الآتية:

3.7.1. كفاءة الكوادر من الجوانب العملية والمهنية والعلمية التخصصية والخبرات والمهارات ذات الصلة.

3.7.2. كفاية الكوادر لإنجاز المهمة، بما يتناسب مع حجم الأعمال اللازمة لإنجاز التدقيق المعلوماتي.

3.7.3. توفر منهجية ودليل تدقيق[1] معياري يتضمن آليات وإجراءات التدقيق وسياسات وإجراءات تقييم الجودة وسياسة تدوير كوادر المدقق المعلوماتي الخارجي ومتطلبات الاستقلالية والموضوعية وسياسة تضمن الالتزام بمعايير السلوك المهني.

3.7.4. تحقيق معايير الاستقلالية والموضوعية ومعايير السلوك المهني التالية:

[1] تفضل المنهجيات التي تستند إلى إطار عمل معياري مثل *COBIT2019* و*معيار CISA* وغيرها من المعايير ذات الصلة التي تصدرها جمعية معايير تدقيق نظم المعلومات *(ISACA) Information Systems Audit and Control Association*.

3.7.4.1. لا يجوز أن يكون المدقق المعلوماتي الخارجي عضواً في مجلس إدارة المؤسسة، أو أن يكون هناك علاقة قرابة حتى الدرجة الثالثة بين أي من كوادر فريق التدقيق المعلوماتي الخارجي وأي من مدراء الإدارات في المؤسسة أو أي من أعضاء مجلس إدارة المؤسسة.

3.7.4.2. لا يجوز أن يعمل أي من كوادر المدقق المعلوماتي الخارجي بصفة دائمة بأي عمل فني أو إداري أو استشاري لصالح المؤسسة.

3.7.4.3. لا يحق للمدقق المعلوماتي الخارجي تنفيذ أكثر من مهمتي تدقيق معلوماتي لمرتين متتاليتين لدى نفس المؤسسة المصرفية.

3.7.4.4. يحظر استفادة المدقق المعلوماتي الخارجي وأياً من فريق التدقيق (وزوجات/ أزواج هؤلاء وأولادهم) من تسهيلات ائتمانية مباشرة وغير مباشرة من المؤسسة المدقق عليها خلال فترة التدقيق ولمدة سنتين لاحقة لها، وتنطبق هذه الأحكام على كفالتهم للغير لقاء تسهيلات ممنوحة من المؤسسة، ويمكن الاستفادة من تسهيلات ائتمانية لغايات شخصية (استهلاكية) بدون أي معاملة تمييزية وشريطة الحصول على موافقة لجنة التدقيق المسبقة في المؤسسة.

3.7.4.5. لا يجوز أن يكون المدقق المعلوماتي الخارجي وكوادره شريكاً مع أي من مديري المؤسسة أو أعضاء مجلس إدارتها أو وكيلاً عنه.

3.7.4.6. لا يجوز أن يكون للمدقق المعلوماتي الخارجي وفريق التدقيق تملك لحصة مؤثرة تتجاوز نسبة 5% من أسهم المؤسسة.

3.7.4.7. لا يجوز أن يكون المدقق المعلوماتي الخارجي وكوادره في علاقة استشارية تخص نطاق المهمة مع المؤسسة أو أي من إداراتها التنفيذية أو أي من أعضاء مجلس إدارتها.

3.7.4.8. لا يجوز أن يتقاضى المدقق من المؤسسة أي مبلغ مالي إضافي سوى البدل المنصوص عليه في العقد المبرم مع المؤسسة بخصوص المهمة.

3.7.4.9. لا يجوز أن يجمع أي من كوادر المدقق المعلوماتي الخارجي بين أعمال التدقيق وأي خدمات إضافية[2] لدى المؤسسة خارج نطاق مهمة التدقيق المكلف بها.

3.7.5. توفر سياسات وإجراءات لدى المدقق المعلوماتي الخارجي تبين الحد الأدنى من المتطلبات الخاصة بكفاءة كوادرها، على أن تشمل الآتي:

3.7.5.1. أن يكون حسن السيرة والسلوك ويتمتع بسمعة مهنية جيدة.

3.7.5.2. ألا يكون محكوم عليه بجناية أو جنحة مخلة بالشرف أو الأمانة.

3.7.5.3. حاصل على شهادة أكاديمية علمية معترف عليها لا تقل عن إجازة جامعية في مجال الاتصالات أو المعلوماتية، وأفضلية توفر شهادة مهنية في مجال التدقيق المعلوماتي من إحدى الجهات المعترف عليها دولياً.

3.7.5.4. توفر خبرة عملية في مجال التدقيق المعلوماتي لمدة لا تقل عن سنتين.

[2] الأعمال التي هي خارجة عن نطاق مهمة التدقيق التي يحددها هذا القرار.

3.7.5.5. توفر المعرفة الكافية بنظم المعلومات المصرفية وخدماتها وتقنياتها ومخاطرها (التقليدية أو الإسلامية) والقوانين والقرارات ذات الصلة.

3.7.5.6. توفر المعرفة الكافية بمعايير التدقيق المعلوماتي الدولية ومعايير السلوك المهني ومستجداتها.

3.7.5.7. ألا يكون قد حرم من مزاولة مهنته أو صدر بحقه حكم جزائي قطعي نتيجة ارتكابه خطأً مهنياً أو مخالفة قانونية ذات علاقة بممارسة المهنة.

3.7.6. توفر سياسة للتدريب المستمر للكوادر لدى المدقق المعلوماتي الخارجي.

3.7.7. توفر الأدوات اللازمة لتنفيذ نشاطات المهمة وكفايتها وكفاءتها.

3.7.8. القدرة على إعداد مخرجات المهمة وتقديمها باللغة العربية (من غير ترجمة).

3.7.9. يجب على المؤسسة إعلام مديرية مفوضية الحكومة لدى المصارف (دائرة التدقيق المعلوماتي) باسم المدقق المعلوماتي الخارجي الذي تم اعتماده خلال أسبوع كحد أقصى من تاريخ توقيع العقد معه، وذلك بموجب كتاب خطي يتضمن معلومات تفصيلية عن المدقق الخارجي وعن كوادره، وعلى أن يكون العقد باللغة العربية.

3.7.10. يجوز للمؤسسة المالية المصرفية التعاقد مع مدقق معلوماتي خارجي سبق وتعاقدت معه لنفس الغاية مع مراعاة البنود المتعلقة بسياسة تدوير المدققين والاستقلالية والموضوعية ومعايير السلوك المهني في هذا القرار.

3.7.11. يجب على مجلس إدارة المؤسسة ولجنة التدقيق التحقق من تمتع المدقق المعلوماتي الخارجي من المعايير المحددة في هذا القرار قبل التعاقد معه، والتأكد من عدم وجود ما يؤثر على مهمة التدقيق وجودتها.

3.7.12. يجب على مجلس إدارة المؤسسة أو/لجنة التدقيق متابعة عمل المدقق المعلوماتي الخارجي خلال تنفيذ المهمة للتأكد بالحد الأدنى مما يلي:

3.7.12.1. فاعلية نشاطات التدقيق في كافة مراحل المهمة من خلال تقييم مدى ملائمة وكفاية أساليب التدقيق ومستوى الأهمية والمخاطر والنشاطات التي لها تأثير محتمل على جميع نظم المعلومات والبنية التقنية المستثمرة لدى المؤسسة.

3.7.12.2. استقلالية وموضوعية المدقق المعلوماتي الخارجي واحترامه لمعايير السلوك المهني.

3.7.12.3. التزام المدقق المعلوماتي الخارجي بنطاق وخطة العمل، والتدقيق في الأسباب التي تؤدي إلى تغييرات أو انحرافات.

3.7.12.4. الاستئناس برأي موظفي المؤسسة المعنيين بالمهمة حول أداء المدقق المعلوماتي الخارجي.

المادة 4 -

4.1. -نطاق مهمة تدقيق نظم المعلومات الخارجية والتقارير المطلوبة:

4.1.1. يجب أن تكون المهمة شاملة لكافة البنى التحتية ونظم تقانة المعلومات المستثمرة في المؤسسة، والتي تشمل بالحد الأدنى ما يلي:

4.1.1.1. نظام المصرف الأساسي ونظم الخدمات المصرفية وكافة النظم الملحقة به أو المرتبطة معه، تقنياً أو وظيفياً.

4.1.1.2. النظم الإدارية والمالية والأمنية وأية نظم ملحقة بها أو المرتبطة معها، تقنياً أو وظيفياً.

4.1.1.3. البنى التحتية والاتصالات ومراكز البيانات الرئيسية والاحتياطية وخطط الاستمرارية ومواجهة الكوارث وحالات الطوارئ.

4.1.2. يجب أن تشمل مهام ونشاطات المهمة مراجعة وتدقيق وتقييم شامل لكافة العمليات المتعلقة بالبنى التحتية ونظم تقانة المعلومات المستثمرة في المؤسسة، وفقاً للأهداف المبينة في المادة (1) من هذا القرار، ويرتبط ذلك بالحد الأدنى ما يلي:

4.1.2.1. الاستراتيجيات والسياسات المكتوبة والمعتمدة على مستوى المؤسسة وعلى مستوى تقانة المعلومات.

4.1.2.2. المعايير والإجراءات والضوابط وقواعد العمل والعمليات والمهام الوظيفية المعتمدة.

4.1.2.3. آليات توظيف الكوادر البشرية على النظم المعلوماتية وأدائها وآليات المراقبة والتأهيل والتطوير.

4.1.2.4. الإشراف على البنى التحتية ونظم تقانة المعلومات المستثمرة لدى المؤسسة.

4.1.2.5. مخاطر البنى التحتية ونظم تقانة المعلومات المستثمرة لدى المؤسسة سواء أكانت من مصادر داخلية أو خارجية.

4.1.2.6. الاستحواذ على البنى التحتية ونظم تقانة المعلومات المستثمرة في المؤسسة وتطويرها وإدارة التغيير.

4.1.2.7. التراخيص وعقود خدمات الدعم الفني وصيانة النظم التقنية (مملوكة أو مستخدمة أو مشغلة) لدى المؤسسة.

4.1.2.8. إدارة خدمات البنى التحتية ونظم تقانة المعلومات المستثمرة في المؤسسة.

4.1.2.9. موثوقية البنى التحتية ونظم تقانة المعلومات المستثمرة في المؤسسة واستمراريتها واستعادتها.

4.1.2.10. أمن المعلومات والتشفير والصلاحيات والسماحيات والتحكم بالدخول.

4.1.2.11. الخدمات المصرفية الإلكترونية وأمن وحماية أدوات وقنوات الدفع الإلكتروني.

4.1.2.12. اختبار أمن النظم التقنية ومراجعة الكود المصدري في حال توفره.

4.1.2.13. مرونة نظام التخزين ووسائطه وتخطيط الاستيعابية.

4.1.2.14. الحماية من حجب الخدمة ومخاطرها.

4.1.2.15. النظم المعلوماتية عبر الانترنت (نظم الخدمات الإلكترونية) والإجراءات الأمنية ذات الصلة.

4.1.2.16. إجراءات التوعية وحماية العملاء.

4.1.2.17. ضوابط وإجراءات حماية مراكز البيانات ومكوناتها المادية والبرمجية.

4.1.2.18. غرفة المخدمات والتجهيزات الموجودة ضمنها (المخدمات – تجهيزات الشبكة الحاسوبية – أجهزة عدم انقطاع التيار الكهربائي (UPS)– أجهزة الحماية من الحريق– كاميرات المراقبة....) وإجراءات الأمان الموجودة فيها.

4.1.3. يجب أن تشمل نشاطات المهمة اختبارات اختراق داخلية وخارجية شاملة لكافة البنى التحتية ونظم تقانة المعلومات المستثمرة في المؤسسة وكافة الخدمات الالكترونية المرتبطة بها، مع تدقيق للإعدادات وتصنيف للأصول المعلوماتية وتحليل للمخاطر حسب الأهمية وأولوية المعالجة.

4.1.4. يجب أن تشمل نشاطات المهمة مراجعة وتدقيق وتقييم شامل لنتائج آخر تقرير تدقيق معلوماتي داخلي و/أو خارجي.

4.1.5. يجب أن تشمل نشاطات المهمة تحليل وتصنيف للمخاطر حسب درجة أهميتها وفق منهجية معيارية عالمية، وأن يتم اقتراح الحلول العلاجية الأمثل وبشكل تفصيلي مع المدة المتوقعة اللازمة لإنجاز المعالجة ونشاطات مهمة إعادة الاختبار والتحقق والجودة.

4.1.6. يجب أن تشمل إجراءات ونشاطات المهمة الأدوات والمعايير الآتية بالحد الأدنى:

4.1.6.1.القوانين السورية وقرارات مجلس الوزراء ومجلس النقد والتسليف ومصرف سورية المركزي والتعاميم ذات الصلة وحسب خصوصية التطبيق وتعديلاتها اللاحقة.

4.1.6.2.يجب أن تشمل مهام ونشاطات المهمة تحليل فجوة للواقع الحالي لنطاق المهمة مع المعايير والقوانين والقرارات النافذة، وتقييم لنقاط الضعف، واقتراح للإجراءات العلاجية المثلى حسب الأهمية وبشكل تفصيلي والمدة المتوقعة اللازمة لإنجاز المعالجة، ونشاطات مهمة إعادة الاختبار والتحقق والجودة.

4.1.6.3.يجب أن يتم تقديم تقرير موحد للمهمة وشامل لكافة النشاطات والإجراءات، باللغة العربية (غير مترجم)، ومبوب حسب المحاور والبنود المبينة في البند 4.1 أعلاه وتوثيق شامل لمصادر المعلومات والوثائق وكافة الأدوات المستخدمة في تنفيذ المهمة، مع شرح لكافة الرموز والدلالات والاختصارات المستخدمة في التقرير والوثائق المرفقة به.

4.2. تقييم التقارير ومعالجة النتائج:

4.2.1. يعتبر مجلس إدارة المؤسسة و/أو لجنة التدقيق-مسؤولاً عن تقييم أداء المدقق المعلوماتي الخارجي المتعاقد معه لتنفيذ مهمة تدقيق نظم المعلومات الخارجية، وفق المعايير المحددة في هذا القرار.

4.2.2. يعتبر مجلس إدارة المؤسسة و/أو لجنة التدقيق مسؤولاً عن متابعة معالجة مخرجات ونتائج التقارير لمهمة التدقيق المعلوماتي وفق خطة عمل تنفيذية تتضمن الإجراءات التفصيلية والتصحيحية والعلاجية مصنفة حسب الأولويات ودرجة الأهمية وفق برنامج زمني محدد وتتم موافاة مديرية مفوضية الحكومة لدى المصارف بهذا البرنامج مع نتائج التتبع والمتابعة.

4.2.3. تقوم مديرية مفوضية الحكومة لدى المصارف بالمتابعة والتدقيق الميداني لاحقاً -إن لزم الأمر- للتأكد من التزام المصرف بإنجاز معالجة نتائج مهمة تدقيق نظم المعلومات الخارجية وفق خطة العمل التنفيذية والإجراءات التصحيحية والعلاجية المعتمدة.

المادة 5 -

5.1. مهلة التدقيق: تلتزم المؤسسة بتدقيق نظم المعلومات من خلال التعاقد مع مدقق معلوماتي خارجي وفقاً لأحكام هذا القرار (مرة على الأقل كل سنتين)، باستثناء اختبارات الاختراق الداخلية والخارجية والمشار إليها في البند 4.1.3 أعلاه حيثُ تلتزم المؤسسة بإجراء هذه الاختبارات بشكل سنوي (مرة على الأقل كل سنة) على مستوى كافة النظم المستثمرة والخدمات المرتبطة بها، كما وتلتزم المؤسسة بإجراء هذه الاختبارات لدى إطلاق كل خدمة الكترونية مصرفية بحيث يكون الاختبار في هذه الحالة على مستوى الخدمة فقط.

5.2. تلتزم المؤسسة بتزويد مديرية مفوضية الحكومة لدى المصارف بتقرير التدقيق المعلوماتي مع الخطة العلاجية والبرنامج الزمني المشار إليه بالبند 4.2.2 أعلاه وذلك خلال شهر كحد أقصى من انتهاء المهمة.

ثانياً: تلتزم المصارف والمؤسسات المالية العاملة في الجمهورية العربية السورية بإجراء أول مهمة تدقيق معلوماتي خارجي وفق الإطار المعياري المشار إليه في أولاً اعتبارا من الشهر الأول من العام 2023.

ثالثاً: تلتزم مديرية مفوضية الحكومة لدى المصارف بتقييم تقارير التدقيق المعلوماتي الخارجي وإعداد تقرير شامل بالنتائج للعرض على مجلس النقد والتسليف.

رابعاً: يبلغ هذا القرار من يلزم لتنفيذه.

رئيس مجلس النقد والتسليف

الدكتور محمد عصام هزيمة

د/أ