ملحق لائحة عمل لجنة إدارة المخاطر

مهام ومسؤوليات لجنة إدارة المخاطر بموجب ضوابط الحوكمة والادارة المؤسسية لتقنية المعلومات والاتصالات في القطاع المصرفي :

أ- وضع استراتيجية، وادارة الأدوار والمسؤوليات في عملية ادارة مخاطر تقنية المعلومات والاتصالات وتوزيعها.

ب- انشاء اطار لمفاهيم ادارة مخاطر تقنية المعلومات والاتصالات بطريقة منتظمة ومنسقة وان يشمل الصفات الاتية:

1. القواعد والمسؤوليات.
2. تحديد وترتيب أولويات اصول نظام المعلومات.
3. تحديد وتقييم التهديدات والمخاطر المحتملة ونقط الضعف الحالية والناشئة.
4. تطبيق المعايير الدولية (ISO 31000, NIST, COBIT for RISK, ISO/IEC 27005:2018, IT GXM).
5. تطبيق الممارسات والرقابة المناسبة للتخفيف من المخاطر.
6. تحديث دوري وتقييم للمخاطر بما يشمل التغييرات في النظم البيئية او الظروف التشغيلية التي قد تؤثر في تحليل المخاطر.

ت- وضع ممارسات فعالة لإدارة المخاطر والرقابة الداخلية لتحقيق سرية البيانات، وأمن النظام، والموثوقية، والمرونة، والقابلية للتعافي في المؤسسة.

ملحق اختصاصات وصلاحيات لجنة التدقيق

مهام ومسؤوليات لجنة التدقيق بموجب ضوابط الحوكمة والادارة المؤسسية لتقنية المعلومات والاتصالات في القطاع المصرفي :

أ- على لجنة التدقيق المنبثقة عن المجلس من جهة والمدقق الخارجي من جهة اخرى، تزويد البنك المركزي العراقي بتقرير سنوي للتدقيق الداخلي، واخر للتدقيق الخارجي على الترتيب يتضمن رد الادارة التنفيذية واطلاع وتوصيات المجلس بشأنه، وذلك بحسب ماورد في البند (د/2) من المادة سادسا (التدقيق الداخلي والخارجي) ووفقاً لنموذج رقم (4) تقرير تدقيق (مخاطر- ضوابط) المعلومات والتقنية ذات الصلة، وذلك خلال الربع الاول من كل عام، وتحل هذه التقارير محل نظيرتها او التي تشملها من التقارير المطلوبة بموجب ضوابط سابقة.

ب- تضمين مسؤوليات عمل تدقيق تقنية المعلومات والاتصالات وصلاحياته، ونطاقه، ضمن ميثاق التدقيق (Audit charter) من جهة، وضمن اجراءات متفق عليها مع المدقق الخارجي من جهة اخرى، وبما يتوافق مع ضوابط الحوكمة المؤسسية لتقنية المعلومات والاتصالات ويغطيها.

ت- التأكد من التزام المدقق الداخلي والمدقق الخارجي للمؤسسة، لدى تنفيذ عمليات التدقيق المختص للمعلومات والتقنية ذات الصلة، وكما مبين في البند (د) من المادة سادسا (التدقيق الداخلي والخارجي)، بما ياتي:

1. معايير تدقيق تقنية المعلومات والاتصالات بحسب اخر تحديث للمعيار الدولي (Information Technology Assurance Framework) (ITAF) الصادر عن جمعية التدقيق والرقابة على نظم المعلومات (ISACA) ومنها:
   - تنفيذ مهمات التدقيق ضمن خطة معتمدة بهذا الشأن تأخذ بالحسبان الاهمية النسبية للعمليات ومستوى المخاطر ودرجة التأثير في اهداف ومصالح المؤسسة.
   - توفير والالتزام بخطط التدريب والتعليم المستمر من قبل الكادر المتخصص بهذا الصدد.
   - الالتزام بمعايير الاستقلالية المهنية والادارية وضمان عدم تضارب المصالح الحالية والمستقبلية.
   - الالتزام بمعايير الموضوعية وبذل العناية المهنية والحفاظ المستمر على مستوى التنافسية والمهنية من المعارف والمهارات الوجب التمتع بها، ومعرفة عميقة في اليات وعمليات المؤسسة المختلفة المرتكزة على تقنية المعلومات والاتصالات وتقارير المراجعة والتدقيق الاخرى (المالية والتشغيلية والقانونية)، والقدرة على تقييم الدليل المتناسب مع الحالة والوضع العام في كشف الممارسات غير المقبولة والمخالفة لاحكام القوانين والانظمة والضوابط.
2. فحص عمليات توظيف وادارة موارد تقنية المعلومات والاتصالات، وتقييمها ومراجعتها، وكذلك عمليات المؤسسة المرتكزة عليها، وابداء رأي عام (Reasonable overall Audit Assurance) حيال مستوى المخاطر الكلي للمعلومات والتقنية ذات الصلة ضمن برنامج تدقيق يشمل في الاقل المحاور المبينة في المرفق رقم (5) على ان يكون تكرار التدقيق للمحاور كافة او جزء منها، حداً ادنى مرة واحدة سنوياً في الاقل في حال تم تقييم المخاطر بدرجة (5 او 4) بحسب سلم تقييم المخاطر الموضح في المرفق رقم (4)، ومرة واحدة كل سنتين في الاقل في حال تم تقييم المخاطر بدرجة (3)، ومرة واحدة كل ثلاث سنوات في الاقل في حال تم تقييم المخاطر بدرجة (2 او 1)، مع مراعاة التغير المستمر في مستوى المخاطر والاخذ بالحسبان التغيرات الجوهرية التي تطرأ على بيئة المعلومات والتقنية ذات الصلة خلال مدد التدقيق المذكورة، على ان يتم تزويد (البنك المركزي العراقي) بتقارير التدقيق لاول مرة بغض النظر عن درجة تقييم المخاطر، وعلى ان تشمل عمليات التقييم للمحاور المذكورة اليات المؤسسة المتبعة، من حيث التخطيط الاستراتيجي ورسم السياسات، والمبادئ واجراءات العمل المكتوبة والمعتمدة، واليات توظيف الموارد المختلفة، بما فيها موارد تقنية المعلومات والاتصالات والعنصر البشري، واليات وادوات المراقبة والتحسين

ملحق اختصاصات وصلاحيات لجنة التدقيق

والتطوير، والعمل على توثيق نتائج التدقيق وتقييمها استنادا الى اهمية الاختلافات ونقط الضعف (الملحوظات)، فضلاً عن الضوابط المفعلة وتقييم مستوى المخاطر المتبقية والمتعلقة بكل منها باستخدام معيار منهجي لتحليل وقياس المخاطر، متضمناً الاجراءات التصحيحية المتفق عليها، والمنوي اتباعها من قبل ادارة المؤسسة بتواريخ محددة للتصحيح، مع الاشارة ضمن جدول خاص الى رتبة صاحب المسؤولية في المؤسسة المسؤول عن ملاحظاته.

3. اجراءات منتظمة لمتابعة نتائج التدقيق للتاكد من معالجة الملحوظات والاختلافات الواردة في تقارير المدقق بالمواعيد المحددة، والعمل على رفع مستوى الاهمية والمخاطر تصعيداً تدريجياً في حال عدم الاستجابة، واعلام المجلس بذلك كلما تطلب الامر.
4. تضمين اليات التقييم السنوي (Performance Evaluation) لكوادر تدقيق تقنية المعلومات والاتصالات بمعايير قياس موضوعية، وبحسب التسلسل الاداري التنظيمي لدوائر التدقيق.