دليل حوكمة تقنية المعلومات

أيار 2021

مصرف الشرق الأوسط العراقي للاستثمار

قائمة المحتويات

*تم تطوير هذ الدليل بناء على تعميم البنك المركزي العراقي المرقم (611/14) والمؤرخ في 2019/04/25 وإطار عمل كوبت 2019 الصادر عن جمعية التدقيق والرقابة على نظم المعلومات ISACA

التاريخ	رقم الإصدار
أيار 2021	مسودة

1.مقدمة

1.1 نظرة عامة على حوكمة وإدارة تقنية المعلومات

تم وضع إطار حوكمة وإدارة تقنية المعلومات في مصرف الشرق الأوسط العراقي للاستثمار لضمان توافق أنشطة تقنية المعلومات مع أهداف العمل وتلبية احتياجات أصحاب المصلحة من خلال التعامل الأمثل مع المخاطر وتحسين الموارد وتحقيق الفوائد. يمثل هذا الدليل لحوكمة وإدارة تقنية المعلومات أهداف مجلس إدارة مصرف الشرق الأوسط العراقي لتمكين إطار/نظام حوكمة تقنية المعلومات استنادًا إلى الممارسة الرائدة COBIT 2019.

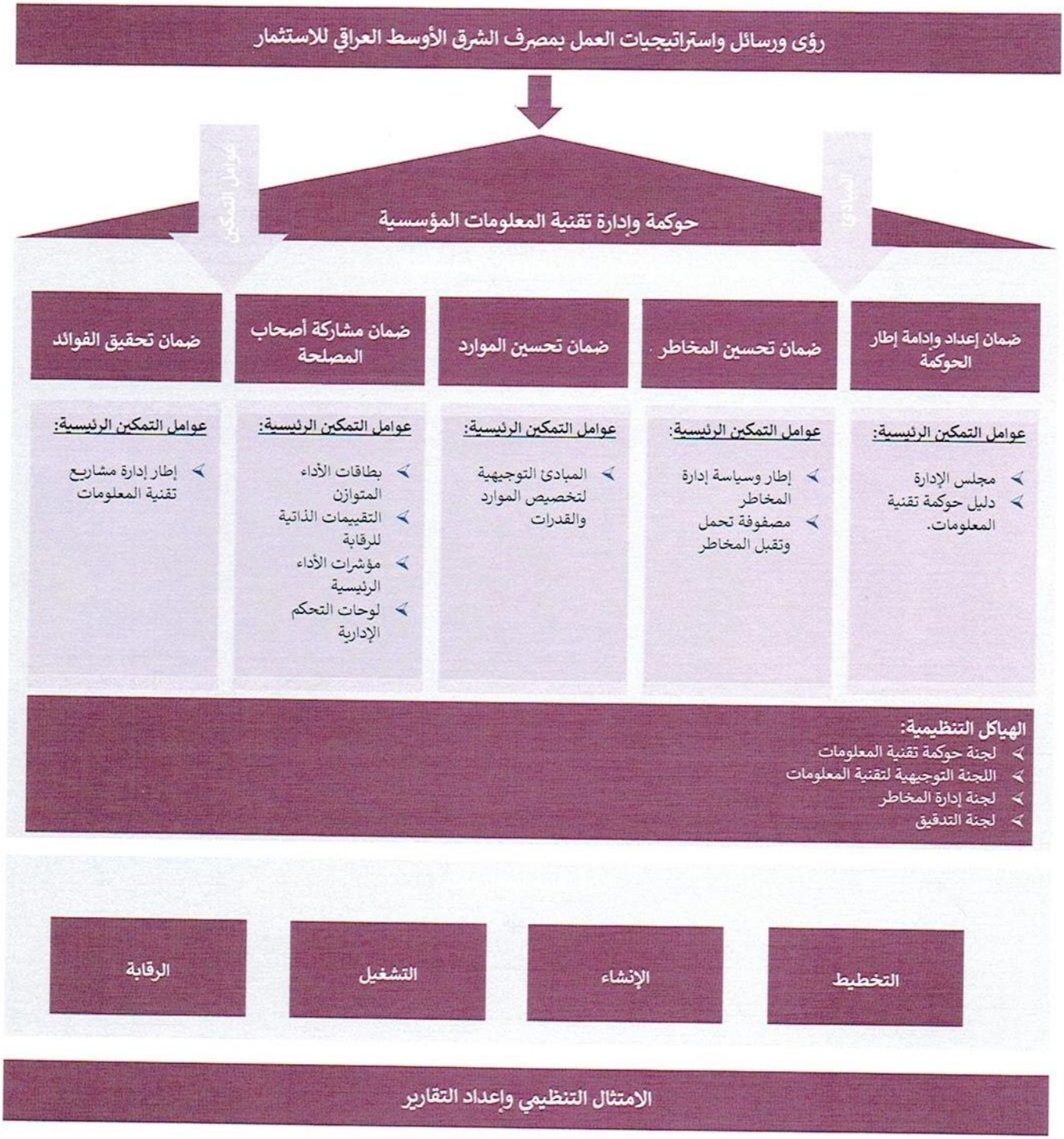
1.2 أهداف حوكمة وإدارة تقنية المعلومات

يهدف إطار حوكمة وإدارة تقنية المعلومات إلى تحقيق الأهداف التالية:

- توافق أهداف تقنية المعلومات مع أهداف العمل.
- تلبية احتياجات أصحاب المصلحة من خلال التعامل الأمثل مع المخاطر، وتحسين الموارد وتحقيق الفوائد.
- تقديم معلومات وتقارير كافية لدعم عملية صنع القرار في مصرف الشرق الأوسط العراقي للاستثمار.
- تحقيق عمليات فعالة لإدارة مشاريع وموارد تقنية المعلومات.
- إنشاء البنية التحتية التقنية ونظم المعلومات التي تمكن من تنفيذ استراتيجيات العمل بالمصرف.
- إدارة مخاطر تقنية المعلومات لضمان الحماية اللازمة لأصول المصرف.
- الامتثال للمتطلبات التنظيمية والقوانين والتشريعات التي تخص ضوابط الرقابة الداخلية والتعليمات والسياسات وإجراءات سير العمل.
- تحسين نظام الرصد والرقابة الداخلية في مصرف الشرق الأوسط العراقي للاستثمار.
- زيادة مستوى رضا المستخدم النهائي عن خدمات تقنية المعلومات.
- إدارة علاقات الأطراف الخارجية/الموردين.

2. حوكمة وإدارة تقنية المعلومات المؤسسية

حدد المصرف خمس عمليات لإطار عمل حوكمة وإدارة تقنية المعلومات، والذي يقوم بدور العنصر الرئيسي لتلبية احتياجات أصحاب المصلحة:



2.1 حوكمة تقنية المعلومات المؤسسية

يلتزم مجلس إدارة مصرف الشرق الأوسط العراقي للاستثمار بتبني منهجية شاملة لضمان الرقابة والإشراف المناسبين على الركائز الخمس المذكورة من خلال تنفيذ الممارسة الأساسية لكوبت COBIT 2019. يتحمل مجلس الإدارة مسؤولية تقييم وتوجيه والرقابة على عمليات الحوكمة في كوبت COBIT 2019 وهو ما يستلزم ما يلي:

- ضمان إعداد وإدامة إطار الحوكمة.
- ضمان تحقيق الفوائد.
- ضمان تحسين المخاطر.
- ضمان تحسين الموارد.
- ضمان مشاركة أصحاب المصلحة.

الهياكل التنظيمية:

لجنة حوكمة تقنية المعلومات:

تتكون لجنة حوكمة تقنية المعلومات من ثلاثة أعضاء من مجلس الإدارة.

النطاق والغرض: يتمثل نطاق وغرض لجنة حوكمة تقنية المعلومات في إدارة أنشطة تقنية المعلومات ومواءمتها مع التوجه الاستراتيجي للمصرف. كما يتمثل الهدف النهائي في ضمان تلبية احتياجات أصحاب المصلحة والذي يشمل تحقيق الفوائد، وتحسين المخاطر وتحسين الموارد.

وتيرة عقد الاجتماعات: تجتمع لجنة حوكمة تقنية المعلومات بشكل ربع سنوي أو حسب الحاجة.

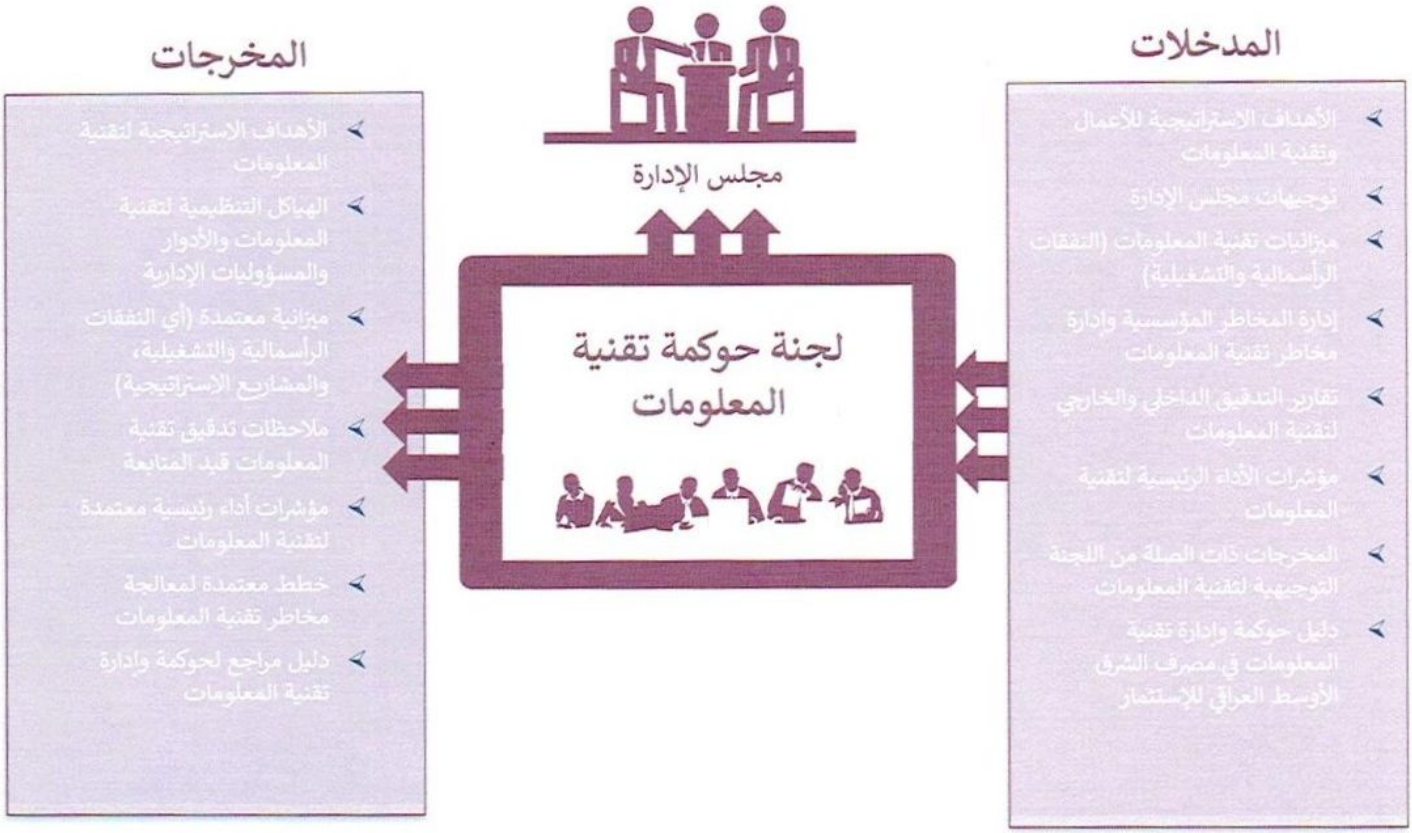
تهدف لجنة حوكمة تقنية المعلومات إلى تحقيق الأهداف التالية:

- ضمان مواءمة الخطط والأهداف الاستراتيجية للمصرف بشكل عام وتقنية المعلومات بشكل خاص.
- رعاية وإدارة التغييرات الاستراتيجية الخاصة بالهيكل التنظيمي للمصرف والمتعلقة بتقنية المعلومات.
- ضمان توافر بيئة عمل وبنية تحتية متكاملة لتقديم مستوى الخدمات المناسبة.
- تشجيع الشفافية والإشراف الفعال على البرامج والمشاريع.
- التأكد من إجراء التدقيق بصورة مستقلة على أنشطة تقنية المعلومات.

الأدوار والمسؤوليات:

- اعتماد الأهداف الاستراتيجية لتقنية المعلومات والهياكل التنظيمية المناسبة بما في ذلك اللجان التوجيهية على مستوى الإدارة التنفيذية العليا وعلى وجه الخصوص (اللجنة التوجيهية لتقنية المعلومات) وبما يضمن تحقيق وتلبية الأهداف الاستراتيجية للمصرف وتحقيق أفضل قيمة مضافة من مشاريع واستثمارات موارد تقنية المعلومات، واستخدام الأدوات والمعايير اللازمة للمراقبة والتأكد من مدى تحقق ذلك.
- اعتماد الإطار العام لإدارة وضبط ومراقبة موارد ومشاريع تقنية المعلومات بما يحاكي أفضل الممارسات الدولية المقبولة بهذا الخصوص وعلى وجه التحديد(COBIT (Control Objectives for Information and related Technology وبما يتوافق مع تعليمات البنك المركز العراقي.
- اعتماد مصفوفة للأهداف المؤسسية، وأهداف المعلومات والتقنية المصاحبة لها، وتوصيف الأهداف الفرعية اللازمة لتحقيقها.
- اعتماد مصفوفة للمسؤوليات RACI Chart تجاه العمليات الرئيسية لحوكمة تقنية المعلومات والعمليات الفرعية المنبثقة عنها من حيث: الجهة أو الجهات أو الشخص أو الاطراف المسؤولة بشكل أولي Responsible، وتلك المسؤولة بشكل نهائي Accountable وتلك المستشارة Consulted، وتلك التي يتم اطلاعها Informed تجاه كافة العمليات.
- التأكد من وجود إطار عام لدى إدارة المخاطر خاص بتقنية المعلومات يتوافق ويتكامل مع الإطار العام الكلي لإدارة المخاطر في المؤسسة وفقا للمعايير الدولية (ISO 31000,ISO 73)
- اعتماد موازنة موارد ومشاريع تقنية المعلومات بما يتوافق مع متطلبات وأهداف استراتيجية للمصرف.

- الاشراف العام ومراقبة سير عمليات وموارد ومشاريع تقنية المعلومات للتأكد من كفايتها ومساهمتها الفاعلة في تحقيق متطلبات وأعمال المصرف.
- الاطلاع على تقارير التدقيق لتقية المعلومات واتخاذ ما يلزم من إجراءات لمعالجة الانحرافات والتوصية للمجلس باتخاذ الاجراءات اللازمة لتصحيح أية انحرافات.
- ضمان استقلالية جميع الأطراف الرئيسية حسب الضرورة لتجنب تضارب المصالح.



المرجعية إلى لجان الحوكمة المؤسسية الحالية:

- لجنة إدارة المخاطر: تتضمن مسؤوليات لجنة إدارة المخاطر إدارة مخاطر تقنية المعلومات ورفع التقارير إلى مجلس الإدارة.
- لجنة التدقيق: تشمل مسؤوليات لجنة التدقيق تقييم فاعلية الضوابط الداخلية لتقنية المعلومات ورفع التقارير الى مجلس الإدارة والبنك المركزي العراقي.

2.2 إدارة تقنية المعلومات المؤسسية

تتحمل الإدارة التنفيذية لتقنية المعلومات مسؤولية تنفيذ رؤية واستراتيجية مجلس الإدارة من خلال ما يلي:

- مواءمة وتخطيط وتنظيم أهداف ومبادرات تقنية المعلومات كما هو موضح في التوجه الاستراتيجي لمجلس الإدارة ورؤيته للأعمال وتقنية المعلومات.
- بناء واكتساب وتنفيذ البنية التحتية والتطبيقات والخدمات اللازمة.
- إدارة وصيانة خدمات الأعمال القائمة.
- مراقبة وتقييم أداء وامتثال جميع عمليات وممارسات وأنشطة تقنية المعلومات المشار إليها تحت مظلة إدارة تقنية المعلومات.

الهياكل التنظيمية

اللجنة التوجيهية لتقنية المعلومات:

تتألف اللجنة التوجيهية لتقنية المعلومات مما يلي:

- المدير المفوض (رئيس اللجنة).
- نائب المدير المفوض (الرئيس البديل للجنة).
- مدير دائرة المخاطر.
- مدير قطاع المعلوماتية.
- مراقبان، وهما أحد أعضاء مجلس الإدارة ورئيس التدقيق الداخلي.
- مدير أمن المعلومات

النطاق والغرض: يتمثل نطاق وغرض اللجنة التوجيهية لتقنية المعلومات في تقديم التوصيات واتخاذ القرارات ودفع المبادرات المتعلقة بتقنية المعلومات لضمان مواءمة الأعمال وتقنية المعلومات، وتحسين القيمة من موارد تقنية المعلومات وتقليل مخاطر تقنية المعلومات.

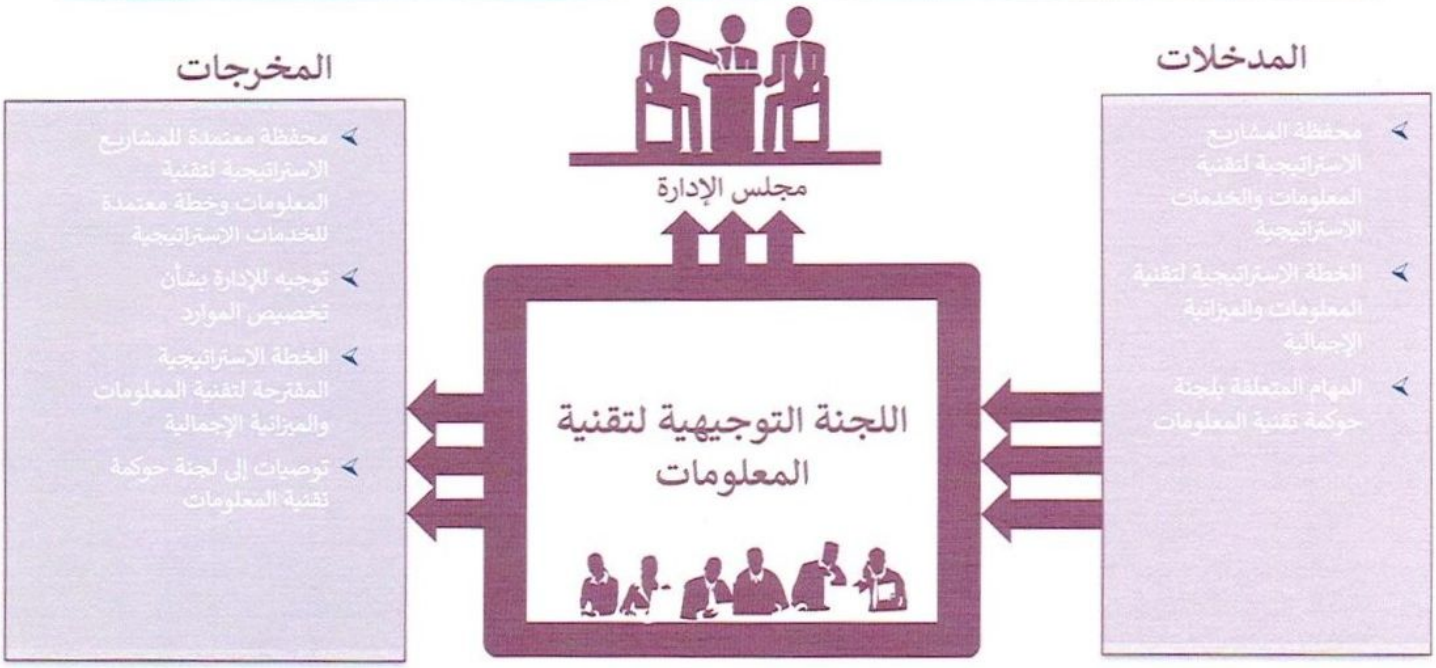
وتيرة عقد الاجتماعات: تجتمع اللجنة التوجيهية لتقنية المعلومات بشكل ربع سنوي أو حسب الاقتضاء، وتعمل تحت إشراف لجنة حوكمة تقنية المعلومات.

تهدف اللجنة التوجيهية لتقنية المعلومات إلى تحقيق الأهداف التالية:

- ضمان تحقيق الأهداف الاستراتيجية لتقنية المعلومات.
- ضمان تحديد أولويات برامج/مشاريع تقنية المعلومات وتنفيذها بشكل صحيح بما يتماشى مع الغرض (الأغراض) الاستراتيجية لأعمالهم.
- الاستخدام الأمثل لموارد تقنية المعلومات.
- تقليل المخاطر في بيئة تقنية المعلومات والرقابة عليها.

الأدوار والمسؤوليات:

- وضع ومراجعة الخطط السنوية لتحقيق الأهداف الإستراتيجية لمجلس الإدارة. بالإضافة إلى الرقابة المستمرة على العوامل الداخلية والخارجية التي قد تؤثر على تحقيق تلك الأهداف.
- ربط أهداف المصرف وأهداف تقنية المعلومات بالمراجعات المنتظمة لضمان تحقيق الأهداف الإستراتيجية للمصرف. يجب أن تحدد اللجنة مجموعة من مؤشرات الأداء الرئيسية لقياس ورصد تحقيق الأهداف باستمرار.
- التوصية بتخصيص الموارد المالية وغير المالية اللازمة لتحقيق أهداف حوكمة تقنية المعلومات.
- إعطاء الأولوية لبرامج ومشاريع تقنية المعلومات.
- مراقبة مستوى أداء خدمات تقنية المعلومات وتقديم توصيات لتحسين فعاليتها وكفاءتها.
- رفع التوصيات اللازمة للجنة حوكمة تقنية المعلومات بشأن ما يلي:
  - تخصيص الموارد والآليات اللازمة لتحقيق أهداف حوكمة تقنية المعلومات.
  - الانحرافات التي قد تؤثر سلبًا على تحقيق الأهداف الاستراتيجية.
  - أي مخاطر غير مقبولة متعلقة بتقنية وأمن المعلومات.
  - تقارير الأداء والامتثال بمتطلبات الإطار العام لإدارة وضبط ومراقبة موارد ومشاريع تقنية المعلومات.



3. المبادئ والمكونات

3.1 مبادئ حوكمة وإدارة تقنية المعلومات

يتم وضع القيم الأساسية لمبادئ نظام حوكمة وإدارة تقنية المعلومات بالمصرف استنادًا إلى مبادئ كوبت COBIT 2019 على النحو التالي:

1. تلبية احتياجات أصحاب المصلحة من خلال خلق القيمة لهم والحفاظ على التوازن بين تحسين المخاطر واستخدام الموارد وتحقيق الفوائد.
2. تغطية المصرف بشكل كامل، وذلك يشمل الالتزام:

- على مستوى مجلس الإدارة من خلال نظام ونطاق حوكمة قوي لتقنية المعلومات بهدف وحيد هو خلق القيمة.
- على مستوى الإدارة من خلال تنفيذ التوجيهات على مستوى مجلس الإدارة من خلال إدارة وتنفيذ الأهداف المتفق عليها، وأخيرًا تقديم تقرير عن حالة العمليات وأنشطة التنفيذ إلى مجلس الإدارة.

3. تطبيق إطار واحد متكامل متوافق مع المعايير الدولية وأفضل الممارسات ذات الصلة.
4. تمكين منهجية شاملة لحوكمة وإدارة تقنية المعلومات من خلال المكونات السبعة التي تشمل:

- المبادئ والسياسات وأطر العمل.
- العمليات.
- الهياكل التنظيمية.
- الثقافة والأخلاق والسلوك.
- المعلومات.
- الخدمات والبنية التحتية والتطبيقات.
- الأفراد والمهارات والكفاءات.

5. فصل الحوكمة عن الإدارة من حيث التفريق بين أدوار ومسؤوليات كل مستوى واللجان ذات الصلة.

3.2 المكونات

المكون الأول: المبادئ والسياسات والأطر

يجب أن يضمن مجلس الإدارة التعبير عن القيم الأساسية للمصرف من خلال "مبادئه" و "سياساته" المتوافرة لتزويد الموظفين بالإرشادات التفصيلية حول كيفية وضع المبادئ حيز التنفيذ. يجب أن تتميز السياسات بالفاعلية والكفاءة وأن تتضمن متطلبات الامتثال. وأخيرًا، يجب على المجلس التأكد من وضع الأطر (النابعة من المبادئ والسياسات) والتي يجب أن تكون حديثة ومفتوحة ومرنة وشاملة.

المكون الثاني: العمليات

يجب أن يضمن مجلس الإدارة وضع عمليات الحوكمة التي تتأثر بسياسات وإجراءات المصرف بحيث يتم وصف وتحديد أهداف العملية لتحقيق النتيجة المرجوة من العملية.

المكون الثالث: الهياكل التنظيمية

يجب أن يضمن مجلس الإدارة تحديث الهياكل التنظيمية بما يتماشى مع اللجان والمبادئ والعمليات المتعلقة بالحوكمة، حيث يجب أن توضح الهياكل التنظيمية تفويض الصلاحيات وإجراءات التصعيد وعملية صنع القرار.

المكون الرابع: الثقافة والأخلاق والسلوك

يجب أن يضمن مجلس الإدارة تمكين الحوكمة داخل المصرف من خلال نشر أو توسيع مفهومه فيما يتعلق بمبادئ "الثقافة والأخلاق والسلوك"، حيث يجب وضع ما يلي:

- القواعد والمعايير
- تطبيق الاتصالات
- الحوافز والمكافآت
- تعيين رواد الأعمال
- عقد جلسات توعية دورية تتعلق بالحوكمة

المكون الخامس: المعلومات

يجب أن يضمن مجلس الإدارة ترجمة المعلومات إلى قدرة على تقديم الخدمات الداخلية والخارجية. كما يجب على مجلس الإدارة التأكد من تحويل المعلومات التي تم جمعها (مثل التقارير، ومؤشرات الأداء الرئيسية) إلى "معرفة" وتحولها في النهاية لخلق "قيمة" للمصرف.

المكون السادس: الخدمات والبنية التحتية والتطبيقات

يجب أن يضمن مجلس الإدارة إنشاء الخدمات والبنية التحتية والتطبيقات المناسبة لدعم ممارسات وعمليات الحوكمة.

المكون السابع: الأفراد والمهارات والكفاءات

يجب أن يضمن مجلس الإدارة توافر الأشخاص المناسبين ذوي المهارات والكفاءات المطلوبة لتطبيق ودعم الممارسات والعمليات المتعلقة بالحوكمة.

4. الامتثال التنظيمي وإعداد التقارير

4.1 الامتثال التنظيمي

التزام مجلس الإدارة بالامتثال التنظيمي:

يجب أن يضمن مجلس الإدارة وضع وإعداد حوكمة وإدارة ممارسات تقنية المعلومات المؤسسية بالتوافق مع لوائح حوكمة وإدارة تقنية المعلومات الصادرة عن البنك المركزي العراقي.

كما يجب أن يتأكد مجلس الإدارة من التزام المصرف بمتطلبات القوانين واللوائح والتعليمات الخارجية المتعلقة بتقنية المعلومات (بما في ذلك البنك المركزي العراقي) بالإضافة إلى السياسات والإجراءات الداخلية المستمدة من القوانين واللوائح الخارجية.

4.2 إعداد التقارير

يجب على لجنة التدقيق تزويد البنك المركزي العراقي بتقرير التدقيق الداخلي السنوي لتقنية المعلومات خلال الربع الأول من كل عام. كما تجري إدارة التدقيق الداخلي عمليات تدقيق لتقنية المعلومات (بما في ذلك كوبت COBIT) استنادًا إلى المعيار الدولي لإطار ضمان تقنية المعلومات (ITAF) وتقديم تقرير إلى لجنة التدقيق حول فاعلية إطار حوكمة تقنية المعلومات.

تضمن لجنة التدقيق أن نطاق ميثاق التدقيق الحالي بإدارة التدقيق الداخلي يشمل عمليات حوكمة وإدارة تقنية المعلومات بالتوافق مع لوائح البنك المركزي العراقي.

كما يجب على المصرف الإفصاح عن وجود "دليل حوكمة وإدارة تقنية المعلومات" والامتثال له (مع البنك المركزي العراقي) ضمن التقرير السنوي للمصرف.

مشاركة التدقيق الخارجي:

يجب على المدقق الخارجي للمصرف إجراء مراجعة مستقلة لإجراءات حوكمة وإدارة تقنية المعلومات التي تطبقها إدارة التدقيق الداخلي (عن طريق خطاب تكليف رسمي) وإبلاغ البنك المركزي العراقي بذلك.