

دليل الحوكمة والإدارة المؤسسية لتقنية المعلومات والاتصالات في القطاع المصرفي

المصرف
الأهلي العراقي

المراجعات

الحدث	التاريخ	جهة اعتماد	رقم النسخة
المؤلف	9 JAN 2020	IT governance committee	1.0
مراجعة	9 June 2022	IT governance committee	2.0
مراجعة	10 October 2023	IT governance committee	3.0
مراجعة	24 July 2024	IT governance committee	4.0
مراجعة	21 June 2025	IT governance committee	5.0

تم تطوير هذا الدليل بناء على تعليمات البنك المركز العراقي عدد 611\14 التاريخ 2019\4\25 وإطار كويت 2019 الصادر عن جمعية التدقيق والرقابة على نظم المعلومات ISACA

المحتويات

1.	المقدمة.....	3
2.	لمحة عامة عن المصرف الأهلي العراق.....	4
3.	نطاق وآلية التطبيق و الاطراف المعنية.....	5
4.	أهداف ضوابط حوكمة تقنية المعلومات و الاتصالات في القطاع المصرفي العراقي.....	5
5.	السياسات العامة.....	6
6.	المبادئ الستة لنظام الحاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها.....	11
7.	وضع الأهداف وتتابعها.....	12
	الملحق أ : منظومة السياسات(حد أدنى).....	12
	الملحق ب: الحد الأدنى من التقارير والمعلومات.....	13
	الملحق ج: الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات.....	14
	التعريفات.....	16

1. المقدمة

يدرك المصرف الأهلي العراقي ممثلاً بمجلس الإدارة وإدارته التنفيذية أهمية تقنية المعلومات والاتصالات كبقية الوحدات المصرفية العاملة في البنك. حيث عمل البنك ممثلاً بمجلس الإدارة وإدارته التنفيذية وكافة وحدات الأعمال سواء كانت وحدات مصرفية وتقنية المعلومات والاتصالات على التعاون والعمل سوياً لضم تقنية المعلومات والاتصالات تحت مظلة الحاكمية وأسلوبها الإداري.

واستجابة لتعليمات البنك المركزي العراقي عدد 611\14 التاريخ 25\4\2019، قام البنك بالمبادرة لإعتماد إطار كويت 2019 لحاكمية وإدارة المعلومات والتقنية المصاحبة لها إمتثالاً للتعليمات الصادرة بهذا الخصوص.

كويت 2019 يوفر إطار شامل يساعد البنك في تحقيق أهدافه المتعلقة بحاكمية وإدارة تقنية المعلومات والاتصالات على مستوى المصرف بشكل كامل. حيث أن هذا الإطار يساعد المصرف بالوصول إلى أعلى درجات الفائدة من تقنية المعلومات من خلال الحفاظ على التوازن بين أعلى فائدة من تقنية المعلومات، والاتصالات، وبأقل المخاطر والموارد . يمكن إطار كويت المصرف من التطبيق الكلي للحاكمية والإدارة لكافة وحدات الأعمال، أي بمعنى آخر تغطية لكافة الأعمال ووظائف تقنية المعلومات والاتصالات ومسؤولياتها في المصرف.

2. لمحة عامة عن المصرف الأهلي العراقي

منذ تأسيسه كشركة مساهمة عامة ضمن القطاع الخاص 1995 حرص المصرف الأهلي العراقي على تقديم مجموعة متكاملة من الخدمات المصرفية للشركات والأفراد في العراق. ونظراً للنجاح الذي حققه البنك ولدعم نموه المستقبلي، فقد تمت زيادة رأس مال البنك من 400 مليون دينار عراقي عند التأسيس ليصل إلى 250 مليار دينار عراقي (215 مليون دولار أمريكي) في كانون الأول 2013 .

وفي عام 2005، قام كابيتال بنك (الأردن) بشراء أغلبية أسهم المصرف الأهلي العراقي (68%)، الأمر الذي مكن المصرف الأهلي العراقي من تطوير منتجاته وخدماته، وتعزيز موطئ قدمه عالمياً وتعزيز الشمول المالي على مستوى البلاد.

بفضل شبكته الواسعة من البنوك المراسلة، يمثل كابيتال بنك بوابة المصرف الأهلي العراقي إلى الاقتصادات العالمية، حيث يسهل إرسال واستقبال الحوالات الداخلية والخارجية، ومنح التسهيلات الائتمانية، وتقديم خدمات التمويل التجاري.

وعلاوة على ما سبق، يمكن للمصرف الأهلي العراقي التداول لصالح عملائه في السوق الأردني وفي الأسواق العالمية من خلال شركة كابيتال للاستثمارات، الذراع الاستثماري لكابيتال بنك – فضلاً عن تقديم خدمات التداول في سوق العراق للأوراق المالية من خلال الشركة التابعة المملوكة له بالكامل، شركة المال العراقي.

3. نطاق وآلية التطبيق والاطراف المعنية

ينطبق هذا الدليل على كافة عمليات المصرف الأهلي العراقي التي تعتمد على تقنية المعلومات والاتصالات بكافة فروع المصرف المحلية و الدولية و الادارة العامة. يجب على كافة أصحاب المصالح مراعاة الإمتثال لهذا الدليل كل حسب مسماه وموقعة الوظيفي. ينطبق هذا الدليل ايضا عند توقيع اتفاقيات الاسناد مع الغير لتوفير الموارد البشرية والخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات بهدف تسخير عمليات البنك والخدمات والبرامج والبنية التحتية المقدمة قبل وأثناء فترة التعاقد، وبما لا يعفي المجلس والإدارة التنفيذية العليا من المسؤولية النهائية لتحقيق متطلبات التعليمات. القائمة أدناه تمثل الأطراف الرئيسية ومسؤولياتها بهذا الخصوص:

- رئيس وأعضاء المجلس والخبراء الخارجيين المستعان بهم: تولي مسؤوليات التوجيه العام للمشروع / البرنامج والموافقة على المهام والمسؤوليات ضمن المشروع، والدعم وتقديم التمويل اللازم .
- المدير المفوض ونوابه ومساعديه ومدراء العمليات والفروع: تولي مسؤوليات تسمية الأشخاص المناسبين من ذوي الخبرة بعمليات البنك لتمثيلهم في المشروع وتوصيف مهامهم ومسؤولياتهم.
- مدير ولجان تكنولوجيا المعلومات التوجيهية ومدراء المشاريع: تولي مسؤوليات إدارة المشروع او البرنامج وتوجيهه والإشراف عليه بشكل مباشر والتوصية بتوفير الموارد اللازمة لإتمامه، والتأكد من الفهم الصحيح من قبل كافة الأطراف بمتطلبات وأهداف التعليمات .
- التدقيق الداخلي: تولي مسؤولياته المناطة به بموجب التعليمات بشكل مباشر، و المشاركة في المشروع / البرنامج بما يمثل دور التدقيق الداخلي في الأمور التنفيذية كمستشار ومراقب مستقل لتسهيل و انجاح إتمام المشروع / البرنامج.
- إدارات المخاطر وأمن المعلومات والامتثال والقانونية: تولي مسؤوليات المشاركة في المشروع البرنامج بما يمثل دور تلك الإدارات، والتأكد من تمثيل المشروع / البرنامج من قبل كافة الأطراف المعنية.
- المتخصصين وحملة الشهادات الفنية والمهنية الخاصة بالإطار (COBIT Assessor, Implementation,) (COBIT Foundation, CGEIT) المستعان بهم من داخل البنك ومن خارجه: تولي دور المرشد لنشر المعرفة بالإطار وتسهيل عملية التطبيق.

4. أهداف ضوابط حوكمة تقنية المعلومات والاتصالات في القطاع المصرفي العراقي

وضع المصرف الأهلي العراقي الأهداف التالية لإطار حاكمية وإدارة المعلومات والتقنية المصاحبه لها:

- 4.1 تلبية احتياجات أصحاب المصالح وتحقيق أهداف المصرف من خلال استخدام إطار حوكمة راسخ النضوج بما يضمن:
 - ادارة حسيصة لموارد ومشاريع تقنية المعلومات والاتصالات للاستفادة من تلك الموارد، وتقليل الهدر فيها.
 - توفير معلومات ذات جودة عالية كمرتكز يدعم آليات صنع القرار في المصرف.
 - يضمن توفير البنية التحتية التكنولوجية التي تمكن المصرف من تحقيق أهدافه.
 - يضمن رفع مستوى العمليات المصرفية وذلك من خلال استخدام وتوظيف أنظمة تكنولوجية فعالة وموثوق بها وأن يتم إختيارها لتحقيق الأهداف المنشودة.
 - يضمن توفير إدارة مخاطر تقنية المعلومات والاتصالات بشكل صارم لضمان الحماية الضرورية واللازمة لموجودات المصرف.

- توفير المساعدة في تحقيق الالتزام بمتطلبات القوانين والتشريعات والضوابط، فضلاً عن الامتثال لاستراتيجية وسياسات وإجراءات العمل الداخلية.
- تحسين نظام الضبط والرقابة الداخلي.
- تعظيم مستوى رضا عن تقنية المعلومات والاتصالات من قبل مستخدميها بتلبية احتياجات العمل بكفاءة وفعالية.
- إدارة خدمات العملاء و الأطراف الخارجية الموكل اليها تنفيذ عمليات و مهام الخدمات والمنتجات المتعلقة بتقنية المعلومات والاتصالات.

4.2 فصل مجلس الإدارة عن الإدارة التنفيذية بما يتوافق وأفضل المعايير والممارسات المعترف بها دولياً لحاكمية وإدارة المعلومات و التقنية المصاحبة لها.

4.3 تبني ممارسات وقواعد العمل والتنظيم بحسب أفضل المعايير الدولية كنقطة إنطلاق يتم الإرتكاز والبناء عليها في مجالي حاكمية و ادارة عمليات ومشاريع وموارد تكنولوجيا المعلومات.

4.4 تعزيز آليات الرقابة الذاتية والرقابة المستقلة وفحص الامتثال في مجالي حاكمية و ادارة المعلومات والتكنولوجيا المصاحبة لها وبما يسهم في تحسين وتطوير الأداء بشكل مستمر.

5. السياسات العامة

5.1 يستند هذا الدليل إلى تعليمات البنك المركزي العراقي عدد 611\14 التاريخ 25\4\2019، وينبغي مراجعة وتحديث هذا الدليل بشكل منتظم وبما يتواءم مع التحديثات التي تطرأ على المصرف.

5.2 يتم اعتماد الدليل من مجلس الادارة. ويقوم المصرف من خلال لجنة حاكمية تقنية المعلومات والاتصالات المنبثقة عن مجلس الإدارة، بمراجعة هذا الدليل وتحديثه عند الضرورة. ويعبر هذا الدليل عن نظرة المصرف الخاصة لحاكمية وادارة المعلومات والتكنولوجيا المصاحبة لها من حيث مفهومها وأهميتها ومبادئها الأساسية.

5.3 يقوم المصرف، بنشر هذا الدليل بأية طريقة مناسبة لاطلاع الجمهور، و يفصح المصرف في تقريره السنوي عن وجود دليل خاص لحوكمة وادارة المعلومات والتقنية المصاحبة لها أو متضمن لدليل الحوكمة المؤسسية لديه، ويفصح أيضاً عن المعلومات التي تهم أصحاب المصالح بما فيها الدليل، وعن مدى التزامه بتطبيق ما جاء فيه.

5.4 اللجان

• لجنة حوكمة تقنية المعلومات والاتصالات:

- تماشياً مع تعليمات البنك المركزي العراقي، قام مجلس الإدارة بتشكيل لجنة من أعضاء مجلس الإدارة تعنى بحوكمة تقنية المعلومات والاتصالات، وتتكون هذه اللجنة من ثلاثة أعضاء على الأقل، وتضم في عضويتها أهل الخبرة والمعرفة في تقنية المعلومات والاتصالات .

- وللجنة الاستعانة عند اللزوم وعلى نفقة المصرف بخبراء خارجيين وذلك بالتنسيق مع رئيس المجلس بغرض تعويض النقص بهذا المجال من جهة ولتعزيز الرأي الموضوعي من جهة أخرى، وللجنة دعوة أي من إداريي المصرف لحضور اجتماعاتها للاستعانة برأيهم بما فيهم المعنيين في التدقيق الداخلي و أعضاء الإدارة التنفيذية العليا مثل مدير تقنية المعلومات والاتصالات أو المعنيين في التدقيق الخارجي، ويحدد المجلس

أهدافها ويفوضها بصلاحيات من قبله، وذلك وفق ميثاق يوضح ذلك، وعلى أن تقوم برفع تقارير دورية للمجلس، علماً بأن تفويض المجلس صلاحيات للجنة أو أي لجنة أخرى لا يعفيه ككل من تحمل مسؤولياته بهذا الخصوص.

- تجتمع هذه اللجنة بشكل ربع سنوي على الأقل، ويتم الاحتفاظ بسجلات ومحاضر الاجتماع وتوثق حسب الأصول. وتتولى المهام التالية:

1- اعتماد الخطط الاستراتيجية لتقنية المعلومات والاتصالات والهيكل التنظيمية المناسبة بما في ذلك اللجان التوجيهية على مستوى الإدارة التنفيذية العليا وعلى وجه الخصوص اللجنة التوجيهية لتقنية المعلومات والاتصالات وبما يضمن تحقيق وتلبية الأهداف الاستراتيجية للمصرف و تحقيق أفضل قيمة مضافة من مشاريع واستثمارات موارد تقنية المعلومات والاتصالات، واستخدام الأدوات والمعايير اللازمة لمراقبة والتأكد من مدى تحقق ذلك، مثل استخدام نظام بطاقات الأداء المتوازن لتقنية المعلومات والاتصالات IT Balanced Scorecards و احتساب معدل العائد على الاستثمار (ROI) وقياس أثر المساهمة في زيادة الكفاءة المالية والتشغيلية.

2- اعتماد الإطار العام لإدارة وضبط ومراقبة موارد ومشاريع تقنية المعلومات والاتصالات بشكل يحاكي أفضل الممارسات الدولية المقبولة بهذا الخصوص وعلى وجه التحديد COBIT بجميع إصداراتها لتحقيق أهداف ومتطلبات هذه الضوابط من خلال تحقيق الأهداف المؤسسية الواردة في المرفق رقم (1) بشكل مستدام، وتحقيق مصفوفة أهداف المعلومات والتقنية المصاحبة لها، الواردة في المرفق رقم (2)، ويغطي عمليات حوكمة تقنية المعلومات والاتصالات الواردة في المرفق رقم (3).

3- اعتماد أهمية وترتيب أولوية أهداف المؤسسة (Enterprise Goals) الواردة في المرفق رقم (1)، وأهداف المعلومات ولتقنية ذات الصلة، الواردة في المرفق رقم (2)، وعدّ معطياتها حدّاً أدنى، وتوصيف الأهداف الفرعية اللازمة لتحقيقها.

4- اعتماد مصفوفة للمسؤوليات RACI CHART تجاه العمليات الرئيسية لحوكمة تقنية المعلومات والاتصالات في المرفق رقم (3)، والعمليات الفرعية المنبثقة عنها من حيث: الجهة أو الجهات أو الشخص أو الأطراف المسؤولة بشكل أولي (Responsible) وتلك المسؤولة بشكل نهائي (Accountable) والأطراف الاستشارية (Consultant) وتلك التي يتم إطلاعها تجاه كل العمليات (Informed) في المرفق المذكور بهذا الشأن.

5- التأكد من وجود إطار عام لإدارة مخاطر تقنية المعلومات والاتصالات يتوافق والإطار العام مع الكلي لإدارة المخاطر في المصرف ويتكامل معه وفقاً للمعايير الدولية مثل (ISO 31000, ISO73) يأخذ بعين الاعتبار ويلبي كافة عمليات حاكمية تقنية المعلومات والاتصالات.

6- اعتماد موازنة موارد ومشاريع تقنية المعلومات والاتصالات بما يتوافق والأهداف الاستراتيجية للمصرف.

7- الاشراف العام والاطلاع على سير عمليات وموارد ومشاريع تقنية المعلومات والاتصالات للتأكد من كفايتها ومساهمتها الفاعلة في تحقيق متطلبات وأعمال المصرف.

8- الإطلاع على تقارير التدقيق لتقنية المعلومات والاتصالات واتخاذ ما يلزم من إجراءات لمعالجة الانحرافات ورفع التوصيات باتخاذ الإجراءات اللازمة لتصحيح أية انحرافات.

• اللجنة التوجيهية لتقنية المعلومات والاتصالات:

قامت الإدارة التنفيذية العليا بتشكيل هذه اللجنة وذلك لضمان تطبيق المواءمة الاستراتيجية بين أهداف تقنية المعلومات والاتصالات لتحقيق الأهداف الاستراتيجية للمصرف وبشكل مستدام، وعليه تم تشكيل لجنة تسمى باللجنة التوجيهية تقنية المعلومات والاتصالات برئاسة المدير المفوض وعضوية مدراء الإدارة التنفيذية العليا بما في ذلك مدير تقنية المعلومات والاتصالات ومدير إدارة المخاطر ومدير أمن المعلومات، وينتخب المجلس أحد أعضائه ليكون عضواً مراقباً في هذه اللجنة بالإضافة لمدير التدقيق الداخلي، ويمكنها دعوة الغير لدى الحاجة لحضور اجتماعاتها.

تجتمع هذه اللجنة بشكل ربع سنوي على الأقل، وتتولى بصورة خاصة القيام بالمهام الآتية:

1. اعداد الخطط الاستراتيجية والتشغيلية لإدارة المخاطر الكفيلة بالوصول الى الأهداف الاستراتيجية المقررة من قبل المجلس والإشراف على تنفيذها لضمان تحقيقها ومراقبة العوامل الداخلية والخارجية المؤثرة فيها بشكل مستمر.
2. ربط مصفوفة الاهداف المؤسسية بمصفوفة اهداف المعلومات و التقنية ذات الصلة، كما وردت في المرفق رقم (2)، واعتمادها ومراجعتها بشكل مستمر، وبما يضمن تحقيق الاهداف الاستراتيجية للمؤسسة واهداف الضوابط، ومراعاة تعريف مجموعة معايير للقياس ومراجعتها وتكليف المعنيين من الادارة التنفيذية بمراقبتها بشكل مستمر واضطلاع اللجنة على ذلك.
3. التوصية بتخصيص الموارد المالية وغير المالية اللازمة لتحقيق الأهداف وعمليات حوكمة تقنية المعلومات والاتصالات، الواردة في المرفقين رقم (2) (3) على الترتيب، حداً أدنى، الاستعانة بالعنصر البشري المناسب من خلال هياكل تنظيمية تشمل كافة العمليات اللازمة لدعم الأهداف تراعي فصل المهام وعدم تضارب المصالح، وتطوير البنية التحتية التقنية والخدمات الأخرى المتعلقة بها خدمة للأهداف، وتولي عمليات الإشراف على سير تنفيذ مشاريع وعمليات حوكمة تقنية المعلومات والاتصالات.
4. ترتيب مشاريع وبرامج تقنية المعلومات والاتصالات بحسب الأولوية.
5. مراقبة مستوى الخدمات الفنية والتقنية والعمل على رفع كفاءتها وتحسينها بشكل مستمر.
6. رفع التوصيات اللازمة للجنة حوكمة تقنية المعلومات والاتصالات بخصوص الأمور التالية:

- تخصيص الموارد اللازمة و الآليات الكفيلة بتحقيق مهام لجنة حاكمية تكنولوجيا المعلومات .
 - أية إنحرافات قد تؤثر سلباً على تحقيق الأهداف الاستراتيجية .
 - أية مخاطر غير مقبولة متعلقة بتقنيات وأمن وحماية المعلومات .
 - تقارير الأداء والامتثال بمتطلبات الإطار العام لإدارة وضبط ومراقبة موارد ومشاريع تقنية المعلومات والاتصالات.
7. تزويد لجنة حاكمية تقنية المعلومات والاتصالات بمحاضر اجتماعاتها أولاً بأول والحصول على ما يفيد الاطلاع عليها.

5.5 منظومة السياسات:

- على المجلس أو من يفوض من لجانه اعتماد منظومة المبادئ والسياسات وأطر العمل اللازمة لتحقيق الإطار العام لإدارة وضبط ومراقبة موارد ومشاريع تقنية المعلومات والاتصالات وبما يلبي متطلبات الأهداف وعمليات حوكمة تقنية المعلومات والاتصالات، الواردة في المرفقين رقم (2) و(3) على الترتيب.
- على المجلس أو من يفوض من لجانه اعتماد المبادئ والسياسات وأطر العمل وعلى وجه الخصوص تلك المتعلقة بإدارة مخاطر تقنية المعلومات والاتصالات، وإدارة أمن المعلومات، وإدارة الموارد البشرية والتي تلبي متطلبات عمليات حاكمية تقنية المعلومات والاتصالات الواردة في المرفق رقم(3).
- على المجلس أو من يفوض من لجانه اعتماد منظومة السياسات اللازمة لإدارة موارد وعمليات حوكمة تقنية المعلومات والاتصالات والواردة بالمرفق رقم (6)، واعتبار منظومة السياسات هذه حداً أدنى مع إمكانية الدمج لتلك السياسات حسب ما تقتضيه طبيعة العمل، وعلى أن يتم تطوير سياسات أخرى مواكبة لتطور أهداف المصرف وآليات العمل.

5.6 المعلومات والبيانات والتقارير:

- يقوم مجلس الإدارة والإدارة التنفيذية العليا بضمان تطوير البنية التحتية والأنظمة اللازمة لتوفير المعلومات والتقارير لمستخدميها بهدف المساهمة في صنع القرار السليم في المصرف.
- يقوم مجلس الإدارة أو الجهات المفوضة بتبني نظم المعلومات والتقارير الواردة في المرفق رقم (7)، وتعتبر هذه الأنظمة الحد الأدنى، ويحدد مالكي هذه المعلومات والتقارير التي يتم من خلالها تحديد سلطة المراجعة والإستخدام وتفويضها حسب الحاجة للعمل.
- يتم مراجعة وتحديث سياسات وتقارير المصرف بانتظام وذلك لتعكس أهداف المصرف وعملياته وفقاً لأفضل الممارسات والمعايير.

5.7 الهيكل التنظيمي:

- على المجلس اعتماد الهياكل التنظيمية (الهرمية واللجان) وعلى وجه الخصوص تلك المتعلقة بإدارة موارد وعمليات ومشاريع تقنية المعلومات والاتصالات، وإدارة لأمن المعلومات، وإدارة الموارد البشرية والتي تلبي متطلبات عمليات حوكمة تقنية المعلومات والاتصالات وتحقيق أهداف المصرف بكفاءة وفعالية.
- يراعى ضمان فصل المهام المتعارضة بطبيعتها ومتطلبات الحماية التنظيمية المتعلقة بالرقابة الثنائية كحد أدنى وكفاية وتحديث الوصف الوظيفي لدى اعتماد وتعديل الهياكل التنظيمية للمصرف.

5.8 الخدمات و البرامج والبنية التحتية لتقنية المعلومات والاتصالات:

- على المجلس أو من يفوض من لجانه والإدارة التنفيذية العليا اعتماد منظومة الخدمات والبرامج والبنية التحتية تقنية المعلومات والاتصالات الواردة بالمرفق رقم (8)، وعد تلك المنظومة حداً أدنى، على أن يتم توفيرها وتطويرها بشكل مستمر لمواكبة تطور أهداف المؤسسة وعملياتها، وبما يوافق أفضل ممارسات الدولية المقبولة بهذا الشأن.

- على المجلس أو من يفوض من لجانه والإدارة التنفيذية العليا اعتماد منظومة الخدمات والبرامج والبنية التحتية لتقنية المعلومات والاتصالات الداعمة والمساعدة لتحقيق عمليات حوكمة تقنية المعلومات والاتصالات، ومن ثم أهداف المعلومات والتقنية المصاحبة لها، والأهداف المؤسسية.

5.9 المعرفة، المهارات، والخبرات:

- على المجلس أو من يفوض من لجانه اعتماد مصفوفة المؤهلات (HC Competences) و سياسات إدارة الموارد البشرية اللازمة لتحقيق متطلبات عمليات حوكمة تقنية المعلومات والاتصالات، الواردة في المرفق رقم (3) ، ومتطلبات هذه الضوابط بشكل عام، ووضع الشخص المناسب في المكان المناسب.
- على إدارة المصرف توظيف العنصر البشري المؤهل والمدرّب من الأشخاص ذوي الخبرة في مجالات إدارة موارد تقنية المعلومات والاتصالات وإدارة المخاطر وإدارة أمن المعلومات وإدارة تدقيق تقنية المعلومات والاتصالات اعتماداً على معايير المعرفة الأكاديمية والمهنية والخبرة العملية باعتراف جمعيات دولية مؤهلة بموجب معايير الاعتماد الدولي للمؤسسات المانحة للشهادات المهنية كل بحسب اختصاصه، على أن يتم إعادة تأهيل وتدريب الكوادر الموظفة حالياً لتلبية متطلبات هذا الدليل.
- على الإدارة التنفيذية في المصرف الاستمرار برغد موظفيها ببرامج التدريب والتعليم المستمر للحفاظ على مستوى من المعارف والمهارات يلبي ويحقق عمليات حوكمة تقنية المعلومات والاتصالات، الواردة في المرفق رقم (3).
- على الإدارة التنفيذية في المصرف تضمين آليات التقييم السنوي للكوادر بمعايير قياس موضوعية تأخذ بعين الاعتبار المساهمة من خلال المركز الوظيفي بتحقيق أهداف المصرف.

5.10 التدقيق الداخلي والخارجي

- على المجلس رصد الموازنات الكافية وتخصيص الأدوات والموارد اللازمة بما في ذلك العنصر البشري المؤهل من خلال أقسام متخصصة بالتدقيق على تقنية المعلومات والاتصالات، والتأكد من أن كل من دائرة التدقيق الداخلي في المصرف والمدقق الخارجي قادرين على مراجعة وتدقيق عمليات توظيف وإدارة موارد ومشاريع تقنية المعلومات والاتصالات وعمليات المصرف المرتكزة عليها. من خلال كوادرات مهنية مؤهلة ومعتمدة دولياً بهذا المجال، حاصلين على شهادات اعتماد مهنية سارية مثل CISA .
- على لجنة التدقيق المنبثقة عن المجلس من جهة والمدقق الخارجي من جهة أخرى تزويد البنك المركزي العراقي بتقرير سنوي للتدقيق الداخلي وآخر للتدقيق الخارجي على التوالي يتضمن رد الإدارة التنفيذية وإطلاع وتوصيات المجلس بخصوصه، وذلك حسب ما ورد في بند (د/2) من هذه المادة ووفقاً للنموذج تقرير تدقيق (مخاطر-ضوابط) المعلومات والتقنية ذات الصلة في المرفق رقم(4)، وذلك خلال الربع الأول من كل عام، وتحل هذه التقارير محل نظيرتها أو التي تشملها من التقارير المطلوبة بموجب ضوابط سابقة.
- على لجنة التدقيق تضمين مسؤوليات وصلاحيات ونطاق عمل تدقيق تقنية المعلومات والاتصالات ضمن ميثاق التدقيق من جهة وضمن إجراءات متفق عليها مع المدقق الخارجي من جهة أخرى.

- على المجلس التأكد ومن خلال لجنة التدقيق المنبثقة عنه من قيام المدقق الداخلي و المدقق الخارجي للمصرف لدى تنفيذ عمليات التدقيق المتخصص للمعلومات و التقنية المصاحبة لها بالإلتزام بما يلي:
- 1- معايير تدقيق تقنية المعلومات والاتصالات بحسب آخر تحديث للمعيار الدولي ITAF الصادر عن جمعية التدقيق والرقابة ISACA ومنها:
 - تنفيذ مهمات التدقيق ضمن خطة معتمدة بهذا الخصوص تأخذ بالحسبان الأهمية النسبية للعمليات ومستوى المخاطر ودرجة التأثير في أهداف ومصالح المصرف.
 - توفير والإلتزام بخطط التدريب والتعليم المستمر من قبل الكادر المتخصص بهذا الصدد.
 - الإلتزام بمعايير الاستقلالية المهنية والإدارية وضمان عدم تضارب المصالح.
 - الإلتزام بمعايير الموضوعية وبذل العناية المهنية والحفاظ المستمر على مستوى التنافسية والمهنية من المعارف والمهارات الواجبة التمتع بها، ومعرفة العميقة في اليات وعمليات المؤسسة المختلفة المرتكزة على تقنية المعلومات والاتصالات وتقارير المراجعة والتدقيق الأخرى.
- 2- فحص وتقييم ومراجعة عمليات توظيف وإدارة موارد تقنية المعلومات والاتصالات عمليات المصرف المرتكزة عليها واعطاء رأي عام حيال مستوى المخاطر الكلي للمعلومات والتقنيات المصاحبة لها ضمن برنامج تدقيق.
- 3- إجراءات منتظمة لمتابعة نتائج التدقيق للتأكد من معالجة الملاحظات والاختلالات الواردة في تقارير المدقق بالمواعيد المحددة. والعمل على رفع مستوى الأهمية والمخاطر تصعيديا تدريجيا في حال عدم الاستجابة ووضع المجلس بصورة ذلك كلما تطلب الأمر.
- 4- تضمين آليات التقييم السنوي لكوادر تدقيق تقنية المعلومات والاتصالات بمعايير قياس موضوعية وعلى أن تتم عمليات التقييم من قبل المجلس ممثلاً بلجنة التدقيق المنبثقة عنه وبحسب التسلسل الإداري التنظيمي لدوائر التدقيق، أو من يحل محلها في المصارف الأجنبية.
- من الممكن إسناد دور المدقق الداخلي للمعلومات والتقنيات المصاحبة لها لجهة خارجية متخصصة مستقلة تماماً عن المدقق الخارجي المعتمد بهذا الخصوص، شريطة تلبية كافة متطلبات هذه التعليمات وأية تعليمات أخرى ذات صلة و احتفاظ لجنة التدقيق المنبثقة عن المجلس والمجلس نفسه بدورهما فيما يتعلق بفحص الامتثال والتأكد من تلبية هذه المتطلبات كحد أدنى.

6. المبادئ الستة لنظام الحاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها

يستند إطار حاكمية المعلومات والتكنولوجيا المصاحبة لها في المصرف الأهلي العراقي إلى ستة مبادئ رئيسية لنظام كوبيت 2019:

1. تحقيق القيمة المرجوة التي تلبي احتياجات أصحاب المصالح من خلال الحفاظ على التوازن بين التعامل الأمثل مع المخاطر، والاستخدام الأمثل للموارد، وتحقيق القيمة.
2. الفصل بين مسؤوليات الحاكمية والإدارة من خلال توزيع الأدوار والمسؤوليات في كل المستويات واللجان ذات الصلة.
3. التغطية الشاملة للبنك.
4. تطبيق إطار عمل صُممَ وتمّ تكيفه ليلبي احتياجات البنك، وذلك من خلال استخدام مجموعة من العناصر التي تأخذ بعين الاعتبار العوامل المؤثرة في تشكيل إطار حاكمية تكنولوجيا المعلومات (COBIT 2019 - Design Factors) بما

يتناسب مع خصوصية واستراتيجيات البنك، لترتيب أهمية وألوية أهداف إدارة وحاكمة التكنولوجيا والمعلومات المصاحبة لها في البنك.

5. تطبيق إطار عمل ديناميكي قابل للتحديث والتطوير لمواكبة التغيرات في المؤسسة. ففي حال تغير أي من عوامل تصميم هذا الإطار (على سبيل المثال تغير في استراتيجية المؤسسة أو التكنولوجيا) يمكن النظر في تأثير هذه التغيرات على نظام الحاكمية في البنك و تحديثه لمواكبة واستيعاب هذه التغيرات وتلبية الاحتياجات الجديدة.

6. تطبيق منهجية شاملة لحاكمة وإدارة تكنولوجيا المعلومات من خلال 7 عناصر تمكين وهي:

- المبادئ والسياسات وأطر العمل.
- عمليات حاكمية تكنولوجيا المعلومات.
- الهياكل التنظيمية.
- المعلومات والتقارير.
- الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات.
- المعارف والمهارات والخبرات.
- منظومة القيم والأخلاق والسلوكيات.

7. وضع الأهداف وتتابعها

تعمل كل مؤسسة في سياق مختلف عن الأخرى ويتم تحديد هذا السياق بواسطة عوامل خارجية وأخرى داخلية. فالعوامل الخارجية تتضمن السياسات العامة للدولة، القوانين، التوزيع الجغرافي، التهديدات والمخاطر الخارجية...الخ؛ أما العوامل الداخلية فتشمل الثقافة، التنظيم، القابلية للمخاطرة...الخ. ويتطلب هذا السياق المؤسسي نظاماً للحوكمة والإدارة يتناسب معه.

يجب أن يتم تحويل إحتياجات أصحاب المصلحة إلى إستراتيجية مؤسسية قابلة للتنفيذ، تشكل أهداف كويت المتكاملة آلية لترجمة إحتياجات أصحاب المصلحة إلى أهداف مؤسسية مجدية قابلة للتنفيذ يتم تخصيصها وفقاً للمطلوب، ويستتبط منها أهداف التوافق. إن هذه الترجمة تتيح وضع أهداف محددة على كل مستوى وفي كل مجال في المؤسسة لدعم الأهداف الشاملة ومتطلبات أصحاب المصلحة وبذلك يتم المواءمة بين إحتياجات المصرف وحلول وخدمات تقنية المعلومات ودعمها بشكل فاعل.

وقد اعتمد المصرف آلية كويت (COBIT) للأهداف المتتالية لترجمة إحتياجات أصحاب المصلحة إلى أهداف محددة وقابلة للتنفيذ. وتتيح هذه الترجمة وضع أهداف محددة على كل مستوى وفي كل مجال من مجالات المصرف لدعم الأهداف العامة ومتطلبات أصحاب المصلحة، وبالتالي تدعم بشكل فعال المواءمة بين إحتياجات المصرف وحلول وخدمات تقنية المعلومات والاتصالات.

الملحق أ : منظومة السياسات (حد أدنى)

* تستند القائمة أدناه إلى تعليمات البنك المركزي العراقي الواردة في المرفق رقم (6)

يعتمد البنك القائمة التالية من الحد الأدنى من السياسات لتنظيم وإدارة العمليات في البنك:

- حوكمة تنظيم تقنية المعلومات والاتصالات
- أمن المعلومات وحمايتها
- أمن بيانات بطاقات الدفع وحمايتها
- خطط استمرارية العمل وخطط التعافي من الكوارث

- إدارة مخاطر تقنية المعلومات والاتصالات
- امتثال تقنية المعلومات والاتصالات (IT Compliance)
- خصوصية البيانات (Data Privacy)
- الاستعانة بخبرات خارجية (Outsourcing)
- إدارة محفظة المشروع (Project Portfolio Management)
- إدارة الموجودات (Asset Management)
- الاستخدام المقبول لموارد تقنية المعلومات والاتصالات
- إدارة التغيير (Change Management)
- أجهزة الحواسيب الرئيسية (Servers)
- أجهزة الكمبيوتر الطرفية
- الأجهزة المحمولة
- إدارة الصلاحيات وامتيازات النفاذ (User Access Management)
- System Development Lifecycle
- إدارة مستوى الخدمات (Service Level Management)
- نسخ الاحتياطي و الاسترجاع (Backup and Restore)
- الاحتفاظ بالبيانات (Retention)
- شراء الأنظمة والتجهيزات (Purchasing)
- النفاذ عن بعد (Remote Access)
- الشبكات (Networks)
- الشبكات اللاسلكية (Wireless Networks)
- أجهزة الحماية (firewalls)
- فحص الاختراق وتحليل الثغرات (Penetration Testing and Vulnerability Assessment)
- مقسم الهاتف العام (Public Branch Exchange)
- مقسم الهاتف الخاص (Private Branch Exchange)

الملحق ب: الحد الأدنى من التقارير والمعلومات

* تستند القائمة أدناه إلى تعليمات البنك المركزي العراقي الواردة في المرفق رقم (7)

سيعتمد البنك قائمة الحد الأدنى من التقارير الوارد أدناه لضمان المحافظة على التقارير السليمة في المصرف، وتعتبر التقارير بمثابة مرساة لعمليات صنع القرار.

- مصفوفة الصلاحيات والامتيازات
- تحليل عوامل مخاطر تقنية المعلومات والاتصالات
- تحليل سيناريو مخاطر تقنية المعلومات والاتصالات
- سجل مخاطر تقنية المعلومات والاتصالات

- جدول المسؤوليات لكل خدمة مقدمة RACI Chart
- ملف مخاطر تقنية المعلومات والاتصالات
- تقرير مخاطر تقنية المعلومات والاتصالات
- خريطة مخاطر تقنية المعلومات والاتصالات
- Risk Universe, Appetite and Tolerance
- مؤشرات المخاطر الرئيسية
- Risk Taxonomy
- Risk and Control Activity Matrix (RCAM)
- موازنة أمن وحماية المعلومات
- MIS Report
- استراتيجية أو منهجية تدقيق تقنية المعلومات والاتصالات
- ميثاق التدقيق
- خطة تدقيق تقنية المعلومات والاتصالات
- مصفوفة المؤهلات
- سجل تدقيق تقنية المعلومات والاتصالات
- ملف تدقيق تقنية المعلومات والاتصالات
- أفضل المعايير الدولية لإدارة موارد ومشاريع تقنية المعلومات والاتصالات ، وإدارة مخاطر تقنية المعلومات والاتصالات ، وأمن وحماية والتدقيق على تقنية المعلومات والاتصالات .

الملحق ج: الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات

* تستند القائمة أدناه إلى تعليمات البنك المركزي العراقي الواردة في المرفق رقم (8)

سيعتمد المصرف قائمة الأنظمة والخدمات والبنية التحتية لتقنية المعلومات والاتصالات التي تدعم المعلومات التالية لتحقيق عمليات حاكمية وإدارة المعلومات والتقنية المصاحبة لها.

- (Incident Management Services) خدمات إدارة الحوادث
- جرد أصول تقنية المعلومات والاتصالات
- التوعية بالممارسات الجيدة لأمن المعلومات
- أمن وحماية البيانات والمعلومات المنطقي
- المراقبة لأمن المعلومات
- برمجيات تدقيق تقنية المعلومات والاتصالات

- الاستضافة وضوابط الأمن المادي والبيئي لغرف الخوادم الرئيسية وغرف الاتصالات والتزويد بالكهرباء
- المعايير والمواصفات القياسية العالمية المعتمدة في إنشاء مراكز البيانات

التعريفات

- **الحوكمة:** تضمن الحوكمة تقييم احتياجات أصحاب المصلحة وشروطهم وخياراتهم من أجل تحديد أهداف متوازنة ومتفق عليها على مستوى المؤسسة يتم تحقيقها؛ وتحديد التوجهات المؤسسية من خلال تحديد الأولويات واتخاذ القرارات؛ ورصد الأداء والامتثال اتجاه الاهداف المتفق عليها.
- **كوبت:** يعرف سابقا بأهداف الرقابة على المعلومات والتقنية ذات الصلة ؛ وتستخدم الآن فقط الان كإسم فقط. هو إطار كامل ومقبول دوليا لحوكمة وإدارة معلومات المؤسسة والتقنية التي تدعم المدراء التنفيذيين في المؤسسة والإدارة في تعريفها وتحقيق أهداف العمل وأهداف التوافق ذات الصلة. يدعم كوبت المؤسسات في تطوير وتنفيذ وتحسين ومراقبة ممارسات الحاكمية والإدارة الجيدة المتعلقة بتقنية المعلومات والاتصالات.
- **العملية:** مجموعة من الممارسات التي تتأثر بسياسات البنك وإجراءاته التي تأخذ مدخلات من عدد من المصادر (بما في ذلك العمليات الأخرى)، تتعالج المدخلات وتنتج المخرجات على سبيل المثال، المنتجات والخدمات.
- **مجلس الإدارة :** مجلس إدارة البنك.
- **الإدارة التنفيذية العليا:** تشمل المدير العام للبنك أو المدير الإقليمي، نائب المدير العام أو نائب المدير الإقليمي، مساعد المدير العام أو المدير الإقليمي المساعد، المدير المالي، مدير العمليات، مدير إدارة المخاطر، رئيس الخزنة (الاستثمار)، مدير الامتثال، وكذلك أي موظف في البنك يتمتع بسلطة تنفيذية موازية لأي من السلطات المذكورة أعلاه، ويرتبط وظيفيا ومباشرة بالمدير العام.
- **أصحاب المصلحة:** أي طرف معني في البنك، مثل المساهمين أو الموظفين أو الدائنين أو العملاء أو الموردين أو الهيئات التنظيمية الخارجية المعنية.