دليل حوكمة تقنية المعلومات والاتصالات

مصرف جيهان للاستثمار والتمويل الاسلامي

قائمة المحتوى

سجل الوثيقة ٥
البيانات الأساسية للوثيقة ٥
أولا: المقدمة ٦
ثانياً:أهداف الدليل ٦
ثالثاً: نطاق الدليل ٨
رابعاً: المصطلحات والتعاريف ٩
خامساً: مرجعية الدليل ١٣
سادساً: آلية نشر الدليل ١٣
سابعاً: لجان حاكمية وتقنية المعلومات والتكنولوجيا المصاحبة لها ١٤
ثامناً: التدقيق الداخلي والخارجي ١٨
تاسعاً: الإطار العام لإدارة مخاطر تقنية المعلومات ٢١
عاشراً: المبادئ والسياسات وأطر العمل ٢٢
حادي عشر: الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات ٢٢
ثاني عشر: منظومة القيم والاخلاق والسلوكيات ٢٣
ثالث عشر: المعلومات والتقارير ٢٣
الرابع عشر: الهياكل التنظيمية ٢٤
الخامس عشر: المعارف والمهارات والخبرات ٢٤
سادس عشر :احكام عامة ٢٥
سابع عشر : اعداد واعتماد الدليل ٢٧

أولا: المقدمة

يسعى القادة الاستراتيجيون بمصرف جيهان للاستثمار والتمويل الإسلامي من خلال التوجه الاستراتيجي للاسترشاد بمبادئ حوكمة تقنية المعلومات والاتصالات كونها تمكن المصرف من تحقيق أهدافه في مجالات حوكمة تقنية المعلومات المؤسسية وادارتها بالإضافة إلى أنها تساعد على تحقيق التوازن بين الاهداف المراد تحقيقها وتقليل مستويات المخاطر الخاصة بتقنية المعلومات والاتصالات.

واستجابة لتعليمات البنك المركزي العراقي بمايخص ضوابط الحوكمة والإدارة المؤسسية لتقنية المعلومات والاتصالات في القطاع المصرفي رقم (٦١١/١٣) بتاريخ (٢٠١٩/٤/٢٥) فقد قام مصرفنا بالمبادرة لاعتماد إطار كوبت ٥ لحاكمية وإدارة تقنية المعلومات والتكنولوجيا المصاحبة لها والاتصالات امتثالاً للتعليمات الصادرة بهذا الخصوص.

إن مصرفنا ومن خلال هذا الدليل يؤكد على ضرورة تحفيز وتقييم الاداء، حيث يتكون الدليل من مجموعة من المرتكزات والمبادئ الاساسية، أولها التوافق الاستراتيجي المطلوب تحقيقه من خلال الأهداف الاستراتيجية لتقنية المعلومات والتي بدورها تساهم في تحقيق الأهداف الاستراتيجية للمصرف.

ثانياً:أهداف الدليل

١. استجابة لتعليمات البنك المركزي العراقي بمايخص ضوابط الحوكمة والإدارة المؤسسية لتقنية المعلومات والاتصالات في القطاع المصرفي رقم (٦١١/١٣) بتاريخ (٢٠١٩/٤/٢٥).

٢. تلبية احتياجات أصحاب المصلحة (Stakeholder's Needs) وتحقيق أهداف المصرف من خلال استخدام إطار حوكمة مؤسسية راسخ النضوج.

- توفير معلومات ذات جودة عالية كمرتكز يدعم آليات صنع القرار في المصرف.
- ضمان توفير البنية التحتية التكنولوجية التي تمكن المصرف من تحقيق أهدافه.
- ضمان رفع مستوى العمليات المصرفية وذلك من خلال استخدام وتوظيف أنظمة تكنولوجية فعالة وموثوق بها وأن يتم اختيارها لتحقيق الأهداف المنشودة.

٣. ضمان توفير إدارة مخاطر تكنولوجيا المعلومات بشكل صارم لضمان الحماية الضرورية واللازمة لأصول المصرف.

٤. تحقيق الشمولية في حوكمة وإدارة تقنية المعلومات والتكنولوجيا المصاحبة لها والاتصالات وذلك من خلال عناصر تمكين (دعامات) سبعة (7 Enablers) تكون مصاحبة ومكملة لخدمات تكنولوجيا المعلومات تتمثل ب:

- المبادئ والسياسات وأطر العمل.
- عمليات حوكمة تقنية المعلومات والاتصالات.
- الهياكل التنظيمية.
- المعلومات والتقارير.
- الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات.
- المعارف والمهارات والخبرات.
- منظومة القيم والاخلاق والسلوكيات وضرورة توفيرها بمواصفات وابعاد محددة لتحقيق وخدمة متطلبات وأهداف المعلومات والتكنولوجيا المصاحبة لها ليس فقط في عمليات تكنولوجيا المعلومات وحسب وانما في كافة عمليات المصرف المرتكزة على المعلومات والتكنولوجيا.

٥. يهدف هذا الدليل الوصول لمستوى نضوج (٣,٢) (بعد ثمانية عشر شهراً بحد أقصى كمرحلة أولى) ومن ثم الوصول إلى مستوى نضوج (٥,٢) (بعد ثلاثة أعوام من تاريخ التعليمات) على ان يتم ارسال تقرير الانجاز المتعلق بالامتثال لتحقيق متطلبات التعليمات كل ستة أشهر موضحاً فيه مستوى الانجاز لكل بند من بنود التعليمات.

ثالثاً: نطاق الدليل

١. يشمل نطاق تطبيق الدليل كافة عمليات المصرف المرتكزة على تكنولوجيا المعلومات بمختلف الفروع والاقسام.

٢. جميع الأطراف (أصحاب المصالح) المعنية بتطبيق الدليل كل بحسب دوره وموقعه .

٣. الاطراف المسؤولة وفقاً لمسؤوليتها الرئيسية على النحو الاتي :

- 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 ومعاونيه ومدراء العمليات والفروع: تولي مسؤوليات تسمية الاشخاص المناسبين من ذوي الخبرة بعمليات المصرف لتمثيلهم في المشروع وتوصيف مهامهم ومسؤولياتهم.
- مدير ولجان تكنولوجيا المعلومات التوجيهية ومدراء المشاريع: تولي مسؤوليات إدارة المشروع /البرنامج وتوجيهه والاشراف عليه بشكل مباشر والتوصية بتوفير الموارد اللازمة لإتمامه، والتأكد من الفهم الصحيح من قبل كافة الاطراف بمتطلبات وأهداف الدليل.
- التدقيق الشرعي الداخلي: تولي مسؤولياته المناطة به بموجب التعليمات بشكل مباشر، والمشاركة في المشروع / البرنامج بما يمثل دور التدقيق الداخلي في الامور التنفيذية كمستشار ومراقب مستقل لتسهيل وانجاح اتمام المشروع / البرنامج.
- ادارات المخاطر وأمن المعلومات والامتثال والقانونية: تولي المسؤوليات المشاركة في المشروع / البرنامج بما يمثل دور تلك الادارات، والتأكد من تمثيل المشروع / البرنامج من قبل كافة الأطراف المعنية.
- المتخصصين وحملة الشهادات الفنية والمهنية الخاصة بالمعيار (COBIT 5 Foundation, COBIT 5 Assessor, COBIT 5 Implementation, CGEIT) والمستعان بهم من داخل البنك ومن خارجه، تولي دور المرشد لنشر المعرفة بالمعيار وتسهيل عملية التطبيق.

رابعاً: المصطلحات والتعاريف

الرقم	المصطلح	التعريف
١.	المصرف	مصرف جيهان للاستثمار والتمويل الإسلامي.
٢.	المجلس	مجلس إدارة مصرف جيهان للاستثمار والتمويل الإسلامي.
٣.	البنك المركزي	البنك المركزي العراقي.
٤.	الشخص ذو العلاقة	جميع الاشخاص الموضحين في أدناه: • الشخص ذو الصلة بموجب المادة (١) من قانون المصارف رقم (٩٤) لسنة ٢٠٠٤ • المدير المفوض أو معاونه بعد تركه للعمل لمدة سنتين. • المدقق الخارجي)مراقب الحسابات الخارجي(طول مدة خدمته وسنتين بعد انتهاء عقده مع المصرف. • أي شخص طبيعي أو اعتباري يرتبط بالمصرف بعلاقة تعاقدية خلال مدة العقد.
٥.	أصحاب المصالح	أي ذي مصلحة في المصرف على سبيل المثال)المودعون و المساهمون والموظفون والدائنون والعملاء والزبائن والجهات الرقابية المعنية والسلطات الحكومية.
٦.	المدير	أي شخص مخول بصلاحيات ويكون مسؤولاً عن مجموعة من المسؤولين في المصرف.
٧.	الإدارة التنفيذية العليا:	تشمل الموظفين رفيعي المستوى كما ورد في المادة (١) من قانون المصارف رقم(٩٤) لسنة(٢٠٠٤) وتوافقاً معه تشمل , المدير المفوض للمصرف أو المدير الإقليمي أو معاون المدير المفوض أو معاون المدير الإقليمي والمدير المالي ومدير قسم العمليات المصرفية الدولية ومدير قسم الخدمات المصرفية المحلية, ومدير قسم إدارة المخاطر ومدير قسم الرقابة والتدقيق الشرعي الداخلي ومدير قسم الخزينة و رئيس قسم الامتثال الشرعي

		و مراقبة الامتثال ومدير الفرع الرئيسي , بالإضافة لأي موظف في المصرف له سلطة تنفيذية موازية لأي من السلطات المذكورة ويرتبط وظيفياً مباشرة بالمدير المفوض.
٨.	أهداف تقنية المعلومات والتكنولوجيا المصاحبة لها	مجموعة الأهداف الرئيسية والفرعية المتعلقة بنشاطات الحاكمية والإدارة للمعلومات والتكنولوجيا المصاحبة لها واللازمة لتحقيق الأهداف المؤسسية.
٩.	الأهداف المؤسسية	مجموعة الأهداف المؤسسية المتعلقة بالحاكمية والإدارة المؤسسية واللازمة لتحقيق احتياجات اصحاب المصالح وأهداف هذا الدليل.
١٠.	عمليات حوكمة تقنية المعلومات	مجموعة الممارسات والنشاطات المنبثقة عن سياسات المؤسسة واللازمة لتحقيق أهداف المعلومات والتكنولوجيا المصاحبة لها.
١١.	إدارة تقنية المعلومات والتكنولوجيا المصاحبة لها	مجموعة الانشطة المستمرة التي تقع ضمن مسؤولية الإدارة التنفيذية وتشمل التخطيط بغرض تحقيق الأهداف الاستراتيجية والتنظيم، ونشاطات البناء والتطوير وعمليات الشراء والتنفيذ و التشغيل و توصيل الخدمات والدعم، ونشاطات المراقبة و القياس والتقييم، لتحقيق الاستمرارية وأهداف المصرف وتوجهاته الاستراتيجية.
١٢.	حوكمة تقنية المعلومات والتكنولوجيا المصاحبة لها	توزيع الأدوار والمسؤوليات وتوصيف العلاقات بين الاطراف والجهات المختلفة وأصحاب المصالح (مثل المجلس والإدارة التنفيذية) بهدف تعظيم القيمة المضافة للمؤسسة باتباع النهج الأمثل الذي يكفل الموازنة بين المخاطر والعوائد المتوقعة، من خلال اعتماد القواعد والاسس والآليات اللازمة لصنع القرار وتحديد التوجهات الاستراتيجية والأهداف في المصرف وآليات مراقبة وفحص امتثال مدى تحققها بما يحقق الاستمرارية وتطور المصرف.
١٣.	On – Site	مكان العملية في نفس بناية الإدارة العامة للمصرف في العراق.

١٤.	Off – Site	مكان العملية في بناية مغايرة لبناية الإدارة العامة للمصرف في العراق لكن بنفس المحافظة.
١٥.	Near – Site	مكان العملية في محافظة مغايرة للمحافظة التي تتواجد فيها الإدارة العامة للمصرف في العراق.
١٦.	Off – shore	مكان العملية في بلد مغاير لبلد الإدارة العامة للمصرف.
١٧.	النسخ الاحتياطي	الملفات والمعدات والبيانات والإجراءات المتاحة للاستخدام في حالة حدوث عطل أو خسارة ، في حالة تدمير النسخ الأصلية أو خارج الخدمة.
١٨.	خطة استمرارية العمل ((BCP))	هي خطة تستخدمها المصرف للاستجابة لإعاقة العمليات التجارية الحيوية. يعتمد على خطة الطوارئ لاستعادة النظم الحرجة.
١٩.	تحليل تأثير الأعمالBIA	عملية لتحديد تأثير فقدان دعم أي مورد. ستحدد دراسة تقييم BIA تصاعد تلك الخسارة. ويستند هذا إلى حقيقة أن الإدارة العليا ، عند توفير بيانات موثوقة لتوثيق التأثير المحتمل للمورد المفقود ، يمكنها اتخاذ القرار المناسب.
٢٠.	المشروع	مجموعة منظمة من الأنشطة المعنية بتقديم قدرة محددة (ضرورية ولكنها ليست كافية ، لتحقيق نتيجة أعمال مطلوبة) للمصرف بناءً على جدول زمني وميزانية متفق عليهما.
٢١.	الاستمرارية	الوقاية من الاضطرابات وتخفيفها والتعافي منها. يمكن أيضًا استخدام المصطلحين "تخطيط استئناف الأعمال" و "تخطيط التعافي من الكوارث" و "التخطيط للطوارئ" في هذا السياق ؛ انهم جميعا التركيز على جوانب الانتعاش الاستمراري.
٢٢.	إدارة التكوين/التهيئة	التحكم في التغييرات على مجموعة من عناصر التكوين (الاعدادات التقنية والتهيئة) على دورة حياة النظام.

٢٣.	مالك البيانات	الفرد (الأفراد) ، عادةً ما يكون مديرًا أو شخص مسؤول ، يتحمل مسؤولية سلامة البيانات المحوسبة وإعداد تقارير دقيقة عنها واستخدامها.
٢٤.	خطة التعافي من الكوارث ((DRP))	مجموعة من الموارد البشرية والمادية والتقنية والإجرائية لاستردادها ، في غضون فترة زمنية محددة وتكلفة ، نشاط توقف بسبب حالة طوارئ أو كارثة
٢٥.	نظم المعلومات ((IS))	مجموعة من الأنشطة الإستراتيجية والإدارية والتشغيلية المشاركة في جمع ومعالجة وتخزين وتوزيع واستخدام التقنيات والتكنولوجيات ذات الصلة. تختلف نظم المعلومات عن تكنولوجيا المعلومات ((IT)) في أن نظام المعلومات يحتوي على مكون تكنولوجيا المعلومات الذي يتفاعل مع مكونات العملية.
٢٦.	الاستقلالية	الحكم الذاتي لمدقق نظم المعلومات والتحرر من تضارب المصالح والتأثير غير المبرر. يجب أن يكون لمدقق نظم المعلومات بالمصرف حرية اتخاذ القرارات الخاصة به والتي تحقق مصلحة العمل بكفاءة وفاعلية .
٢٧.	اللجنة التوجيهية لتكنولوجيا المعلومات	لجنة على مستوى الإدارة التنفيذية تساعد في تنفيذ استراتيجية تكنولوجيا المعلومات ، وتشرف على الإدارة اليومية لتقديم خدمات تكنولوجيا المعلومات ومشاريع تكنولوجيا المعلومات ، وتركز على جوانب التنفيذ
٢٨.	الخطة الاستراتيجية لتكنولوجيا المعلومات	هي خطة طويلة الأجل (أي أفق من ثلاث إلى خمس سنوات) والتي تصف فيها إدارة الأعمال وتكنولوجيا المعلومات بشكل تعاوني كيف ستساهم موارد تكنولوجيا المعلومات في تحقيق الأهداف الاستراتيجية للمصرف.
٢٩.	لجنة إستراتيجية تكنولوجيا المعلومات	لجنة على مستوى مجلس الإدارة لضمان مشاركة المجلس في المسائل والقرارات الرئيسية لتكنولوجيا المعلومات. تكون اللجنة مسؤولة بشكل أساسي عن إدارة محافظ الاستثمارات الممكّنة لتكنولوجيا المعلومات

		وخدمات تكنولوجيا المعلومات وغيرها من موارد تكنولوجيا المعلومات. اللجنة هي صاحب الحافظة.
٣٠.	ضمان الجودة ((QA))	نمط مخطط ومنتظم لجميع الإجراءات اللازمة لتوفير ثقة كافية في أن العنصر أو المنتج يتوافق مع المتطلبات الفنية المحددة.
٣١.	الفصل بين المهام ((SOD))	عبارة عن رقابة داخلية أساسية تمنع أو تكتشف الأخطاء والمخالفات عن طريق إسناد فصل الأفراد عن مسؤولية بدء المعاملات وتسجيلها وحفظ الأصول. يستخدم الفصل / الفصل بين الواجبات عادة في مؤسسات تكنولوجيا المعلومات الكبيرة بحيث لا يكون هناك أي شخص في وضع يمكنه من تقديم كود احتيالي أو خبيث دون اكتشاف.

خامساً: مرجعية الدليل

١. **تم انشاء هذه الدليل استجابة لتعليمات البنك المركزي العراقي بمايخص ضوابط الحوكمة والإدارة المؤسسية لتقنية المعلومات والاتصالات في القطاع المصرفي رقم (٦١١/١٣) بتاريخ (٢٠١٩/٤/٢٥) ،و استناداً لأفضل الممارسات الدولية المتبعة بالخصوص.**

سادساً: آلية نشر الدليل

- يقوم المصرف، بنشر هذا الدليل على الموقع الإلكتروني للمصرف ومن خلال أي طريقة مناسبة متاحة لاصحاب المصلحة.
- الإفصاح بالتقرير السنوي عن الدليل ومدى الالتزام بتطبيق ماورد فيه.

سابعاً: لجان حاكمية وتقنية المعلومات والتكنولوجيا المصاحبة لها

أولاً: لجنة حوكمة تقنية المعلومات والاتصالات.

التشكيل:

- تتشكل هذه اللجنة من ثلاثة أعضاء من مجلس الإدارة على الأقل، ويفضل أن تضم في عضويتها أشخاص من ذوي الخبرة أو المعرفة الاستراتيجية في تكنولوجيا المعلومات، 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 إداري المصرف لحضور اجتماعاتها للاستعانة برأيهم بما فيهم المعنيين في التدقيق الداخلي واعضاء الإدارة التنفيذية العليا (مثل مدير قسم 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، علما بأن تفويض المجلس صلاحيات للجنة أو أي لجنة أخرى لا يعفيه ككل من تحمل مسؤولياته بهذا الخصوص، وتجتمع اللجنة بشكل ربع سنوي على الأقل، وتحتفظ بمحاضر اجتماعات موثقة.

- تقوم لجنة الحوكمة المؤسسية المنبثقة عن مجلس بمهام اللجنة بصفة مؤقته لمدة لاتتجاوز ثلاث سنوات من تاريخ اعتماد الدليل.

مهام اللجنة:

١. 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 والاتصالات)، وبما يضمن تحقيق وتلبية الأهداف الاستراتيجية للمصرف وتحقيق أفضل قيمة مضافة من مشاريع واستثمارات موارد تقنية المعلومات والاتصالات، واستخدام الأدوات والمعايير اللازمة للمراقبة والتأكد من مدى تحقق ذلك، مثل استخدام نظام بطاقات الأداء المتوازن لتقنية المعلومات (IT Balanced Scorecards) واحتساب معدل العائد على الاستثمار (ROI) ، وقياس أثر المساهمة في زيادة الكفاءة المالية والتشغيلية.

٢. اعتماد الاطار العام لإدارة وضبط ومراقبة موارد ومشاريع تقنية المعلومات يحاكي أفضل الممارسات الدولية المقبولة بهذا الشأن وعلى وجه التحديد (COBIT)، يوافق ويلبي تحقيق أهداف ومتطلبات المصرف.

٣. اعتماد مصفوفة الأهداف المؤسسية وأهداف المعلومات والتكنولوجيا المصاحبة لها واعتبار معطياتها حداً أدنى، وتوصيف الأهداف الفرعية اللازمة لتحقيقها.

٤. اعتماد مصفوفة للمسؤوليات (RACI Chart) تجاه العمليات الرئيسية لحاكمية تكنولوجيا المعلومات والعمليات الفرعية المنبثقة عنها من حيث: الجهة أو الجهات أو الشخص أو الأطراف المسؤولة بشكل أولي (Responsible) وتلك المسؤولة بشكل نهائي (Accountable)، وتلك المستشارة (Consulted)، وتلك التي يتم اطلاعها (Informed) تجاه كافة العمليات مسترشدين بمعيار (COBIT 5 Enabling Processes) بهذا الخصوص.

٥. التأكيد من وجود إطار عام لإدارة مخاطر تقنية المعلومات والاتصالات يتوافق ويتكامل مع الإطار العام الكلي لإدارة المخاطر في المصرف ويتكامل معه، وفقاً للمعايير الدولية مثل (ISO 31000. ISO 73) ويأخذ بعين الاعتبار جميع عمليات حوكمة تقنية المعلومات ، ويلبيها.

٦. اعتماد موازنة موارد ومشاريع تقنية المعلومات بما يتوافق والأهداف الاستراتيجية للمصرف.

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

٨. الاطلاع على تقارير التدقيق لتقنية المعلومات والاتصالات، واتخاذ ما يلزم من إجراءات لمعالجة الانحرافات ورفع التوصيات باتخاذ الإجراءات اللازمة لتصحيحها.

ثانياً: اللجنة التوجيهية لتقنية المعلومات والاتصالات (IT Steering Committee):

التشكيل:

١. يتم تشكيل اللجنة برئاسة المدير المفوض وعضوية مدراء الإدارة التنفيذية العليا بما في ذلك مدير تكنولوجيا المعلومات ومدير إدارة المخاطر ومدير أمن المعلومات وينتخب المجلس أحد أعضائه ليكون عضواً مراقباً في هذه اللجنة بالإضافة لمديرقسم الرقابة و التدقيق الشرعي الداخلي، ويمكنها دعوة الغير لدى الحاجة لحضور اجتماعاتها، وتوثق اللجنة اجتماعاتها بمحاضر اصولية، على أن تكون دورية الاجتماعات مرة كل ثلاثة أشهر على الاقل.

مهام اللجنة:

١. وضع الخطط السنوية الكفيلة بالوصول للأهداف الاستراتيجية المقرة من قبل المجلس، والاشراف على تنفيذها لضمان تحقيقها ومراقبة العوامل الداخلية والخارجية المؤثرة عليها بشكل مستمر.

٢. ربط مصفوفة الأهداف المؤسسية بمصفوفة أهداف المعلومات والتكنولوجيا المصاحبة لها واعتمادها ومراجعتها بشكل مستمر وبما يضمن تحقيق الأهداف الاستراتيجية للمصرف وأهداف الدليل، ومراعاة تعريف مجموعة معايير للقياس ومراجعتها وتكليف المعنيين من الإدارة التنفيذية بمراقبتها بشكل مستمر واطلاع اللجنة على ذلك.

٣. التوصية بتخصيص الموارد المالية وغير المالية اللازمة لتحقيق الأهداف وعمليات حاكمية تكنولوجيا المعلومات، والاستعانة بالعنصر البشري الكفوء والمناسب في المكان المناسب من خلال هياكل تنظيمية تشمل كافة العمليات اللازمة لدعم الأهداف تراعي فصل المهام وعدم تضارب المصالح، وتطويع البنية التحتية التكنولوجية والخدمات الاخرى المتعلقة بها خدمة للأهداف وتولي عمليات الاشراف على سير تنفيذ مشاريع وعمليات حاكمية تقنية المعلومات والاتصالات.

٤. ترتيب مشاريع وبرامج تتقنية المعلومات حسب الاولوية.

٥. مراقبة مستوى الخدمات الفنية والتكنولوجية والعمل على رفع كفاءتها وتحسينها بشكل مستمر.

٦. رفع التوصيات اللازمة للجنة حاكمية تكنولوجيا المعلومات بخصوص الامور التالية:

- تخصيص الموارد اللازمة والآليات الكفيلة بتحقيق مهام لجنة حاكمية تكنولوجيا المعلومات.
- أية انحرافات قد تؤثر سلبا على تحقيق الأهداف الاستراتيجية.
- أية مخاطر غير مقبولة متعلقة بتكنولوجيا المعلومات.
- تقارير الأداء والامتثال بمتطلبات الإطار العام لإدارة وضبط ومراقبة موارد ومشاريع تكنولوجيا المعلومات.

٧. تزويد لجنة حوكمة تقنية المعلومات والاتصالات (لجنة الحوكمة المؤسسية،حالياً) بمحاضر اجتماعاتها اولا بأول والحصول على ما يفيد الاطلاع عليها.

٨. مراجعة المخاطر الخاصة بإدارة المعلومات والتكنولوجيا المصاحبة لها بما في ذلك المخاطر التي تم تنسيبها من قبل اللجنة التوجيهية لأمن المعلومات ورفع التوصيات للجان المعنية.

ثامناً: التدقيق الداخلي والخارجي

أ- على المجلس رصد الموازنات الكافية وتخصيص الادوات والموارد اللازمة بما في ذلك العنصر البشري المؤهل من خلال أقسام متخصصة بالتدقيق على تقنية المعلومات والاتصالات، والتأكد من أن كلاً من قسم الرقابة و التدقيق الشرعي الداخلي في المصرف والمدقق الخارجي قادران على مراجعة عمليات توظيف وإدارة موارد ومشاريع تقنية المعلومات والاتصالات وإدارتها وعمليات المصرف المرتكزة عليها، مراجعة فنية متخصصة من خلال كوادر مهنية مؤهلة ومعتمدة دولياً في هذا المجال، حاصلين على شهادات اعتماد مهنية سارية مثل (CISA) من جمعيات دولية مؤهلة بموجب معايير الاعتماد الدولي للمؤسسات المانحة للشهادات المهنية (ISO/IEC 17024) و/أو أية معايير أخرى موازية.

ب-على لجنة التدقيق المنبثقة عن المجلس من جهة والمدقق الخارجي من جهة اخرى تزويد البنك المركزي العراقي بتقرير سنوي للتدقيق الداخلي، وآخر للتدقيق الخارجي على الترتيب يتضمن رد الإدارة التنفيذية واطلاع وتوصيات المجلس بشأنه، وفق نموذج تقرير تدقيق (مخاطر -ضوابط) المعلومات والتقنية ذات الصلة ، وذلك خلال الربع الاول من كل عام.

ج-على لجنة التدقيق تضمين مسؤوليات وصلاحيات ونطاق عمل تدقيق تقنية المعلومات ضمن ميثاق التدقيق (Audit charter) من جهة وضمن اجراءات متفق عليها مع المدقق الخارجي من جهة اخرى، وبما يتوافق مع الدليل.

د- على المجلس التأكد من خلال لجنة التدقيق المنبثقة عنه من قيام المدقق الداخلي والمدقق الخارجي للمصرف، لدى تنفيذ عمليات التدقيق المتخصص للمعلومات والتقنية ذات الصلة، بما يأتي:

- معايير تدقيق تقنية المعلومات 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 متعمدة بهذا الشأن تأخذ بالحسبان الأهمية النسبية للعمليات ومستوى المخاطر ودرجة التأثير على أهداف ومصالح المصرف.
- توفير والالتزام بخطط التدريب والتعليم المستمر من قبل الكادر المتخصص بهذا الصدد.
- الالتزام بمعايير الاستقلالية المهنية والإدارية وضمان عدم تضارب المصالح الحالية والمستقبلية.
- الالتزام بمعايير الموضوعية وبذل العناية المهنية والحفاظ المستمر على مستوى التنافسية والمهنية من المعارف والمهارات الواجب التمتع بها، ومعرفة عميقة في آليات وعمليات المصرف المختلفة المرتكزة على تقنية المعلومات والاتصالات وتقارير المراجعة والتدقيق الأخرى (المالية والتشغيلية والقانونية)، والقدرة على تقييم الدليل المتناسب مع الحالة والوضع العام في كشف الممارسات غير المقبولة والمخالفة لأحكام القوانين والانظمة و الضوابط.
- فحص وتقييم ومراجعة عمليات توظيف وإدارة موارد تكنولوجيا المعلومات وعمليات االمصرف المرتكزة عليها واعطاء رأي عام (Reasonable Overall Audit Assurance) حيال مستوى المخاطر الكلي للمعلومات والتكنولوجيا المصاحبة لها ضمن برنامج تدقيق، على أن يكون تكرار التدقيق لكافة المحاور أو جزء منها كحد ادنى مرة واحدة سنوياً على الأقل في حال تم تقييم المخاطر بدرجة (٥ أو ٤) بحسب سلم تقييم المخاطر ومرة واحدة كل سنتين على الاقل في حال تم تقييم المخاطر بدرجة (٣)، ومرة واحدة كل ثلاث سنوات على الاقل في حال تم تقييم المخاطر بدرجة (٢ أو ١)، مع مراعاة التغيير المستمر في مستوى المخاطر والاخذ بعين الاعتبار التغييرات الجوهرية التي تطرأ على بيئة المعلومات والتكنولوجيا المصاحبة لها خلال فترات التدقيق المذكورة، على ان يتم تزويد البنك المركزي بتقارير التدقيق لأول مرة بغض النظر عن درجة تقييم المخاطر، وعلى ان تشمل عمليات التقييم للمحاور المذكورة

آليات المصرف المتبعة من حيث التخطيط الاستراتيجي ورسم السياسات والمبادئ واجراءات العمل المكتوبة والمعتمدة وآليات توظيف الموارد المختلفة بما فيها موارد تكنولوجيا المعلومات والعنصر البشري، وآليات وأدوات المراقبة والتحسين والتطوير والعمل على توثيق نتائج التدقيق وتقييمها اعتمادا على اهمية الاختلالات ونقاط الضعف (الملاحظات) بالإضافة للضوابط المفعلة وتقييم مستوى المخاطر المتبقية والمتعلقة بكل منها باستخدام معيار منهجي لتحليل وقياس المخاطر، متضمنا الاجراءات التصحيحية المتفق عليها والمنوي اتباعها من قبل إدارة المصرف بتواريخ محددة للتصحيح، مع الاشارة ضمن جدول خاص الى رتبة صاحب المسؤولية في المصرف مالك كل ملاحظة.

- إجراءات منتظمة لمتابعة نتائج التدقيق للتأكد من معالجة الملاحظات والاختلافات الواردة في تقارير المدقق بالمواعيد المحددة، والعمل على رفع مستوى الأهمية والمخاطر تصعيداً تدريجياً في حال عدم الاستجابة، وإعلام المجلس بذلك كلما تطلب الأمر.
- تضمين آليات التقييم السنوي (Performance Evaluation) لكوادر تدقيق تقنية المعلومات بمعايير قياس موضوعية، وعلى أن تتم عمليات التقييم من قبل المجلس ممثلا بلجنة التدقيق المنبثقة عنه وبحسب التسلسل الاداري التنظيمي لاقسام التدقيق.

هـ-من الممكن إسناد مهمة المدقق الداخلي للمعلومات والتقنية ذات الصلة (Internal IT Audit) إلى جهة خارجية مختصة مستقلة تماماً عن المدقق الخارجي المعتمد بهذا الشأن (Outsourcing)، شريطة تلبية كافة متطلبات هذه الضوابط وأية ضوابط أخرى ذات صلة، واحتفاظ لجنة التدقيق المنبثقة عن المجلس والمجلس نفسه بوظيفتها، فيما يتعلق بفحص الامتثال والتأكد من تلبية هذه المتطلبات كحد أدنى.

تاسعاً: الإطار العام لإدارة مخاطر تقنية المعلومات

- يجب إنشاء إطار لمفاهيم إدارة مخاطر تقنية المعلومات والاتصالات بطريقة منتظمة ومنسقة. وأن يشمل الصفات التالية:

١. القواعد والمسؤوليات.

٢. تحديد وترتيب أولويات أصول النظام.

٣. تحديد وتقييم التهديدات والمخاطر المحتملة ونقاط الضعف الحالية والناشئة.

٤. تطبيق المعايير الدولية (IT, ISO/IEC 27005:2018, COBIT for RISK, NIST, ISO 31000 GXM).

٥. تطبيق الممارسات والرقابة المناسبة للتخفيف من المخاطر.

٦. تحديث دوري وتقييم للمخاطر بما يشمل التغييرات في النظم البيئية أو الظروف التشغيلية التي قد تؤثر على تحليل المخاطر.

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

- الإشراف على مخاطر تقنية المعلومات والاتصالات من قبل مجلس الإدارة والإدارة العليا من خلال تطبيق القواعد والمسؤوليات:

- إنشاء إطار قوي ومتين لإدارة مخاطر التقنية. ويجب أيضاً أن تتم مشاركة القرارات الاستراتيجية والهامة لتقنية المعلومات فيما بينهم.
- يكون مسؤول بشكل كامل عن فاعلية الرقابة الداخلية وممارسات إدارة المخاطر لتحقيق الأمن والموثوقية والمرونة وقابلية التعافي.
- يجب الأخذ بالحسبان لقضايا التكاليف والفوائد، بما في ذلك عوامل مثل السمعة وثقة الزبائن والأثر المترتب والآثار القانونية، المتعلقة بالاستثمار في عمليات الرقابة وإجراءات الحماية الخاصة لكل من انظمة الحاسوب والشبكات ومراكز البيانات ("DC") وعمليات وتسهيلات النسخ الاحتياطي.

عاشراً: المبادئ والسياسات وأطر العمل

١. اعتماد منظومة المبادئ والسياسات وأطر العمل(Frameworks) اللازمة لتحقيق الإطار العام لإدارة وضبط ومراقبة موارد ومشاريع تقنية المعلومات وبما يلبي متطلبات الأهداف وعمليات حوكمة تقنية المعلومات(المجلس أو من يفوض من لجانه).

٢. اعتماد المبادئ والسياسات وأطر العمل وعلى وجه الخصوص تلك المتعلقة بإدارة مخاطر تكنولوجيا المعلومات، وإدارة أمن المعلومات، وإدارة الموارد البشرية والتي تلبي متطلبات عمليات حوكمة تقنية المعلومات(المجلس أو من يفوض من لجانه).

٣. اعتماد منظومة السياسات اللازمة لإدارة موارد وعمليات حوكمة تقنية المعلومات، واعتبار منظومة السياسات هذه حداً أدنى مع إمكانية الجمع والدمج لتلك السياسات حسب ما تقتضيه طبيعة العمل، وعلى أن يتم تطوير سياسات أخرى ناظمة مواكبة لتطور أهداف المصرف وآليات العمل، وعلى أن تحدد كل سياسة الجهة المالكة ونطاق التطبيق ودورية المراجعة والتحديث وصلاحيات الاطلاع والتوزيع والأهداف والمسؤوليات واجراءات العمل المتعلقة بها، والعقوبات في حالة عدم الامتثال وآليات فحص الامتثال(المجلس أو من يفوض من لجانه).

٤. عند انشاء السياسات يجب مساهمة كافة الشركاء الداخليين والخارجيين واعتماد أفضل الممارسات الدولية وتحديثاتها كمراجع لصياغة تلك السياسات مثل:

(COBIT5, ISO/IEC 27001/2, ISO 31000, ISO/IEC 38500, ISO/IEC 9126, ISO/IEC 15504, ISO 22301, PCI. DSS, ITIL,...etc)

حادي عشر: الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات

١. اعتماد منظومة الخدمات والبرامج والبنية التحتية لتقنية المعلومات الداعمة والمساعدة لتحقيق عمليات حوكمة تقنية المعلومات وبالتالي أهداف المعلومات وتكنولوجيا المصاحبة لها، وبالتالي الأهداف المؤسسية(المجلس او من يفوض من لجانه والإدارة التنفيذية العليا).

٢. اعتماد منظومة الخدمات والبرامج والبنية التحتية لتقنية المعلومات، وعلى ان يتم توفيرها وتطويرها بشكل مستمر لمواكبة تطور أهداف وعمليات المصرف وبما يتفق وأفضل الممارسات الدولية المقبولة بهذا الخصوص(المجلس او من يفوض من لجانه والإدارة التنفيذية العليا).

ثاني عشر: منظومة القيم والاخلاق والسلوكيات

١. اعتماد منظومة اخلاقية مهنية مؤسسية تعكس القواعد السلوكية المهنية الدولية المقبولة بخصوص التعامل مع تقنية المعلومات والتكنولوجيا المصاحبة لها تحدد بوضوح القواعد السلوكية المرغوبة وغير المرغوبة وتبعاتها(المجلس أو من يفوض من لجانه).

٢. الامتثال لمنظومة الاخلاق والممارسات المهنية المعتمدة من قبل المجلس بحيث تتضمن بالحد الادنى منظومة الاخلاق المهنية الواردة في المعيار الدولي (ITAF) الصادر عن جمعية التدقيق والرقابة على نظم المعلومات (ISACA) وتحديثاته(المدقق الداخلي والمدقق الخارجي).

٣. توظيف الاليات المختلفة لتشجيع تطبيق السلوكيات المرغوبة وتجنب السلوكيات غير المرغوبة من خلال اتباع اساليب الحوافز والعقوبات على سبيل المثال لا الحصر(المجلس والإدارة التنفيذية العليا).

ثالث عشر: المعلومات والتقارير

١. تطوير البنية التحتية ونظم المعلومات اللازمة لتوفير المعلومات والتقارير لمستخدميها كمرتكز لعمليات اتخاذ القرار في المصرف، وعليه يجب ان تتوفر متطلبات جودة المعلومات (Information Quality Criteria) والمتمثلة بالمصداقية (Integrity Completeness, Accuracy and Validity or Currency) ومتطلبات السرية بحسب سياسة تصنيف البيانات ومتطلبات التوافرية والامتثال بتلك المعلومات والتقارير، بالإضافة للمتطلبات الاخرى الواردة في المعيار (COBIT 5 – Enabling Information) والمتمثلة بال (Objectivity, Believability, Reputation, Relevancy, Appropriate Amount, Concise Representation, Consistent

Representation, Interpretability, Understandability, Ease of Manipulation, Restricted Access).

٢. على المجلس أو من يفوض من لجانه اعتماد منظومة المعلومات والتقارير، وإعتبار تلك المنظومة حداً أدنى، مع مراعاة تحديد مالكين لتلك المعلومات والتقارير تحدد من خلالهم وتفوض صلاحيات الاطلاع والاستخدام بحسب الحاجة للعمل والشركاء المعنيين، وعلى ان يتم مراجعتها وتطويرها بشكل مستمر لمواكبة تطور أهداف وعمليات المصرف وبما يتفق وأفضل الممارسات الدولية المقبولة بهذا الخصوص.

الرابع عشر: الهياكل التنظيمية

١. تحقيق الرقابة الثنائية كحد أدنى من خلال فصل المهام المتعارضة بطبيعتها ومتطلبات الحماية التنظيمية وتحديث بطاقات الوصف الوظيفي لدى اعتماد وتعديل الهياكل التنظيمية للمصرف.

٢. بما يخص إدارة موارد وعمليات ومشاريع تقنية المعلومات والاتصالات ، وإدارة مخاطر تكنولوجيا المعلومات، وإدارة أمن المعلومات، وإدارة الموارد البشرية لتحقيق أهداف المصرف بكفاءة وفعالية،اعتماد هياكل تنظيمية (هرمية واللجان).

الخامس عشر: المعارف والمهارات والخبرات

١. استقطاب وتعيين الموارد البشرية ذات الكفاءة والمهارة والخبرة في مجالات إدارة موارد تكنولوجيا المعلومات وإدارة المخاطر وإدارة امن المعلومات وإدارة تدقيق تكنولوجيا المعلومات اعتمادا على معايير المعرفة الاكاديمية والمهنية والخبرة العملية باعتراف جمعيات دولية مؤهلة بموجب معايير الاعتماد الدولي للمؤسسات المانحة للشهادات المهنية (ISO/IEC 17024) و/أو أية معايير أخرى موازية كل بحسب اختصاصه، على ان يتم اعادة تأهيل وتدريب الكوادر الحالية لتلبية المتطلبات.

٢. اعداد خطة تدريب للموارد البشرية الحالية تتضمن برامج التدريب والتعليم المستمر للحفاظ على مستوى من المعارف والمهارات يلبي ويحقق حوكمة تقنية المعلومات.

٣. اعتماد آليات التقييم السنوي (Performance Evaluation) للموارد البشرية بمعايير قياس موضوعية تأخذ بعين الاعتبار المساهمة من خلال المركز الوظيفي بتحقيق أهداف المصرف

٤. اعتماد مصفوفة المؤهلات (HR Competencies) وسياسات إدارة الموارد البشرية اللازمة لتحقيق متطلبات عمليات حوكمة تقنية المعلومات، وضمان الاختيار المناسب للمركز الوظيفية بالمصرف.

سادس عشر :احكام عامة

- يُعمل بهذا الدليل اعتبارا من تاريخ إقراره وتُلغى كافة السياسات والتعليمات السابقة المتعلقة بهذا الخصوص.
- يخضع هذا الدليل للمراجعة مرة واحدة كل عامين كحد أدنى أو كلما دعت الحاجة لذلك.

- تعتبر السياسات والمواثيق المذكورة ادناه جزءاً لايتجزء من الدليل :

التسلسل	الوصف
1.	سياسة أمن المعلومات .
2.	ميثاق اللجنة التوجيهية لتقنية المعلومات والاتصالات المنبثقة عن الادارة التنفيذية العليا.
3.	ميثاق لجنة حوكمة تقنية المعلومات والاتصالات المنبثقة عن مجلس الادارة.
4.	سياسة إدارة الصلاحيات وامتيازات النفاذ.
5.	سياسة إدارة مستوى الخدمات.
6.	سياسة الاجهزة المحمولة.
7.	سياسة الاستخدام المقبولة.
8.	سياسة النفاذ عن بعد.
9.	سياسة تحليل الثغرات وفحص الاختراق.

10.	سياسة مقسم الهاتف.
11.	سياسة تطوير/اقتناء الانظمة والبرمجيات.
12.	سياسة الشبكات.
13.	سياسة الشبكات اللاسلكية.
14.	سياسة النسخ الاحتياطي.
15.	سياسة المشتريات وقواعد شراء الاجهزة والانظمة.
16.	سياسة ادارة الوصول .
17.	سياسة الاحتفاظ بالبيانات.
18.	سياسة الاستعانة بمصادر خارجية.
19.	سياسة الجدر النارية.
20.	سياسة أمن بطاقات الدفع وحمايتها.
21.	سياسة اجهزة الكمبيوتر الطرفية.
22.	سياسة ادارة اصول تكنولوجيا المعلومات.
23.	سياسة ادارة التغييرات .
24.	سياسة ادارة المشاريع ومحافظها.

Uncontrolled Copy
وینەی کۆنترۆل نەکراو
CIHAN BANK

الاختصار	المصطلح
APO	Align, Plan, Organize.
CGEIT	Certified in the Governance of Enterprise IT.
CISA	Certified Information System Auditor.
COBIT	Control Objective for Information and Related Technologies.
DSS	Delivery, Service, Support.
EDM	Evaluate, Direct, Monitor.
IEC	International Electrotechnical Commission.
ISACA	Information System Audit and Control Association.
ISO	International Organization for standardization.
ITAF	Information Technology Assurance Framework.
ITIL	Information Technology Infrastructure Library.