دليل حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها

بنك الإسكان

الإصدار الثالث

الفهرس

أولاً: المقدّمة

تعتبر موارد تكنولوجيا المعلومات مرتكزا مهما من حيث الحجم النسبي ومن حيث التأثير على قدرة المؤسسة في تسيير عملياتها وبالتالي تحقيق أهدافها، كما وتلعب دورا حساسا في التأثير على تنافسية منتجات وخدمات المؤسسة من جهة، وعلى آليات صنع القرار وإدارة المخاطر من جهة أخرى، وهذا يبرر حجم الاستثمارات الضخمة في قطاع تكنولوجيا المعلومات من قبل المؤسسات المصرفية. وعليه كان لا بد لبنك الاسكان أن يقوم باتباع المرتكزات والمعايير السليمة في إدارة موارد تكنولوجيا المعلومات بحسب الممارسات الدولية المقبولة بهذا الخصوص لتقليل مخاطرها وتجنبا للدخول في استثمارات غير مجدية ومصاريف غير مبررة تترجم إلى خسائر طائلة تمتد عبر السنوات والتي قد تنال في بعض الأحيان من سمعة المؤسسة، ومن منطلق اهتمام بنك الاسكان بتطبيق قواعد ومرتكزات الحاكمية المؤسسية فقد ارتأى إعداد دليل خاص بحاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها، يكمّل دليل حاكمية المؤسسة وينسجم مع تعليمات البنك المركزي الخاصة بتعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم 2016/65 والصادرة بتاريخ 2016/10/25، وتعليمات الحاكمية المؤسسية للبنوك رقم 2016/63 بتاريخ 2016/9/1 وتعديلاتها اللاحقة، وتعميم البنك المركزي رقم 984/6/10 بتاريخ 2019/1/21 الذي اعتمد الاطار المرجعي COBIT 2019.

يعتمد دليل حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها على المعايير الدولية والمبادىء الرئيسية التي وردت في تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم 2016/65 والتعميم 984/6/10 وعلى الإطار (COBIT) واطار حاكمية أنظمة وتكنولوجيا المعلومات IT Governance Framework والصادر عن جمعية التدقيق والرقابة على نظم المعلومات في الولايات المتحدة الأمريكية Information Systems Audit and Control Association (ISACA) من خلال عدة محاور أهمّها ضرورة تحقيق الأهداف الاستراتيجية **(Strategic Alignment)** من خلال ضمان التوافق الاستراتيجي لأهداف تكنولوجيا المعلومات مع الأهداف الاستراتيجية للمؤسسة والتأكّد من توظيف موارد تكنولوجيا المعلومات بالشكل الأمثل **(Resource Optimization)** وتحقيق الفائدة **(Value Delivery)** وتعظيم القيمة المضافة **(Value Added)** مقاسة بشكل رئيسي بمعيار مساهمة عمليات تكنولوجيا المعلومات في تحقيق أهداف المؤسسة الاستراتيجية والعمل على إدارة مخاطر تكنولوجيا المعلومات**(IT Risk Management)** بشكل متكامل ينسجم وعمليات إدارة المخاطر الكلية للمؤسسة التي تؤدي إلى آليات سليمة لصنع القرارات المرتكزة على المخاطر واعداد وتفعيل مؤشرات قياس الأداء **(Performance Measurement)**، مع مراعاة مبدأ فصل المهام والأدوار وتوزيعها بشكل سليم بين المجلس من جهة والإدارة التنفيذية من جهة أخرى.

ثانياً: الإسناد:

صدر دليل حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها كجزء مكمل لدليل الحاكمية المؤسسية وذلك التزاما بتطبيق تعليمات البنك المركزي المتعلقة بحاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم 2016/65 تاريخ 2016/10/25 وتعميم البنك المركزي رقم 984/6/10 تاريخ 2019/1/21.

ثالثاً: التعريفات:

يكون للكلمات والعبارات الواردة في هذا الدليل المعاني المحددة لها فيما بعد ما لم تدل القرينة أو السياق على غير ذلك، ويتم الرجوع إلى قانون البنوك والتعليمات الصادرة بموجبه بشأن أية تعريفات أخرى ترد في هذا الدليل غير مدرجة في هذا البند:

أ. **الحاكمية المؤسّسية:** النظام الذي يُوجَّه ويدار به البنك، والذي يهدف إلى تحديد الأهداف المؤسّسية للبنك وتحقيقها، وإدارة عمليات البنك بشكل آمن، وحماية مصالح المودعين، والالتزام بالمسؤولية الواجبة تجاه المساهمين وأصحاب المصالح الآخرين، والتزام البنك بالتشريعات وسياسات البنك الداخلية.

ب. **حاكمية المعلومات والتكنولوجيا المصاحبة لها:** توزيع الأدوار والمسؤوليات وتوصيف العلاقات بين الأطراف والجهات المختلفة وأصحاب المصالح (مثل المجلس والإدارة التنفيذية) بهدف تعظيم القيمة المضافة للمؤسسة باتباع النهج الأمثل الذي يكفل الموازنه بين المخاطر والعوائد المتوقعة، من خلال اعتماد القواعد والأسس والآليات اللازمة لصنع القرار وتحديد التوجهات الاستراتيجية والأهداف في البنك وآليات مراقبة وفحص امتثال مدى تحققها بما يكفل ديمومة وتطور البنك.

ج. **إدارة المعلومات والتكنولوجيا المصاحبة لها:** مجموعة النشاطات المستمرة التي تقع ضمن مسؤولية الإدارة التنفيذية وتشمل التخطيط بغرض تحقيق الأهداف الاستراتيجية بما يشمل المواءمة والتنظيم، ونشاطات البناء والتطوير بما يشمل الشراء والتنفيذ، ونشاطات التشغيل بما يشمل توصيل الخدمات والدعم، ونشاطات المراقبة بما يشمل القياس والتقييم، وبما يكفل ديمومة تحقيق أهداف البنك وتوجهاته الاستراتيجية.

د. **اهداف حاكمية وادارة تكنولوجيا المعلومات** :مجموعة الأهداف التي تسعى المؤسسة لتحقيقها من خلال الممارسات والنشاطات المنبثقة عن سياسات المؤسسة واللازمة لتحقيق أهداف المعلومات والتكنولوجيا المصاحبة لها وتوافقها مع الأهداف المؤسسية.

هـ. **أهداف المعلومات والتكنولوجيا المصاحبة لها** – اهداف التوافق: مجموعة الأهداف الرئيسية والفرعية المتعلقة بنشاطات الحاكمية والإدارة للمعلومات والتكنولوجيا المصاحبة لها واللازمة لتحقيق الأهداف المؤسسية.

و. **الأهداف المؤسسية** Enterprise Goals: مجموعة الأهداف المتعلقة بالحاكمية والإدارة المؤسسية واللازمة لتحقيق احتياجات أصحاب المصالح وأهداف تعليمات البنك المركزي بهذا الخصوص.

ز. **المجلس:** مجلس إدارة البنك.

ح. **الإدارة التنفيذية العليا:** تشـــمل الرئيس التنفيذي ورؤســـاء المجموعات ومدير دائرة المخاطر والمدقق العام ومدير دائرة مراقبة الامتثال، ومدراء الدوائر والقطاعات، بالإضـافة لأي موظف في البنك له سـلطة تنفيذية موازية لأي من سلطات أي من المذكورين ويرتبط وظيفياً مباشرة بالرئيس التنفيذي.

ط. **أصحاب المصالح:** أي ذي مصلحة في البنك مثل المودعين أو المساهمين أو الموظفين أو الدائنين أو العملاء أو المزودين الخارجيين أو الجهات الرقابية المعنية.

ي. **التعليمات:** تعليمات البنك المركزي المتعلقة بحاكمية وإدارة المعلومات والتكنولوجيا المصـــاحبة لها رقم 2016/65 والصادرة بتاريخ 2016/10/25 وتعميم البنك المركزي اللاحق رقم 948/6/10 بتاريخ 2019/1/21

ك. **المدقق:** الشـــخص (الطبيعي او المعنوي) او الجهة المختصـــة بفحص عمليات البنك المرتكزة على تكنولوجيا المعلومات وبما ينســـجم مع متطلبات التعليمات بهذا الخصـــوص والمتفق معه من قبل إدارة البنك لتحقيق تلك المتطلبات لفترة لا تقل عن 3 سنوات متتالية ولا تزيد عن 6 سنوات متتالية.

ل. **المرفقـات/الملاحق:** هي المرفقـات الواردة في تعليمـات البنـك المركزي المتعلقـة بحـاكميـة وإدارة المعلومـات والتكنولوجيا المصـاحبة لها رقم 2016/65 والصـادرة بتاريخ 2016/10/25 وعددها ثمانية مرفقات على شـكل ملاحق مطلوب تطبيقها بالتوافق مع المواد –خمسـة عشـرة مادة – الواردة في وثيقة التعليمات الرئيسـية بالإضـافة الى وثائق اطار العمل المرجعي COBIT 2019 والمعتمد حســـب تعميم البنك المركزي رقم 948/6/10 بتاريخ 2019/1/21.

رابعاً: نشر دليل حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها:

يقوم البنك بنشـر هذا الدليل على موقعه الالكتروني، وبأي طريقة أخرى مناسـبة لاطلاع الجمهور، كما يتم الإفصـاح في التقرير السنوي للبنك عن وجود دليل لحاكمية وإدارة المعلومـات والتكنولوجيـا المصـاحبة لهـا، والافصـاح ايضـاً عن المعلومات التي تهم اصحاب المصالح بما فيها الدليل، وعن مدى التزام البنك بتطبيق ما جاء فيه.

خامساً: اللجان:

تم تشكيل لجنتين أحدهما على مستوى مجلس الادارة وتسمى "لجنة حاكمية تكنولوجيا المعلومات" والاخرى على مستوى الادارة التنفيذية العليا وتسمى "اللجنة التوجيهية لتكنولوجيا المعلومات":

أ. لجنة حاكمية تكنولوجيا المعلومات:

- تتشكل هذه اللجنة من ثلاثة اعضاء من مجلس الادارة على الاقل.
- تضم في عضويتها اشخاص من ذوي الخبرة او المعرفة الاستراتيجية في تكنولوجيا المعلومات.
- تقوم اللجنه بالاستعانة – عند اللزوم – وعلى نفقة البنك بخبراء خارجيين وذلك بالتنسيق مع رئيس المجلس بفرض تعويض النقص بهذا المجال من جهة ولتعزيز الرأي الموضوعي من جهة اخرى.

- للجنة دعوة اي من إداري البنك لحضـــور اجتماعاتها للاســـتعانة برأيهم، بما فيهم المعنيين في التدقيق الداخلي واعضاء الادارة التنفيذية العليا (مثل: مدير دائرة انظمة المعلومات) او المعنيين في التدقيق الخارجي.
- يحدد المجلس اهدافها ويفوضها بصلاحيات من قبله، وذلك وفق ميثاق يوضح ذلك.
- تقوم برفع تقارير دورية للمجلس، علماً بأن تفويض المجلس صـــلاحيات للجنة لا يعفيه ككل من تحمل مسـؤولياته بهذا الخصوص.
- تجتمع اللجنة بشكل ربع سنوي على الاقل، وتحتفظ بمحاضر اجتماعات موثقة.
- تتولى اللجنة – كحد أدنى – المهام التالية:

1. اعتماد الأهداف الاستراتيجية لتكنولوجيا المعلومات واهداف التوافق والهياكل التنظيمية المناسبة بما في ذلك اللجان التوجيهية على مستوى الإدارة التنفيذية العليا وعلى وجه الخصوص (اللجنة التوجيهية لتكنولوجيا المعلومات) وبما يضمن تحقيق وتلبية الأهداف الاستراتيجية للبنك وتحقيق أفضل قيمة مضافة من مشاريع واستثمارات موارد تكنولوجيا المعلومات، واستخدام الأدوات والمعايير اللازمة لمراقبة والتأكد من مدى تحقق ذلك، مثل استخدام نظام بطاقات الأداء المتوازن لتكنولوجيا المعلومات (IT Balanced Scorecards) واحتساب معدل العائد على الاستثمار (Return On Investment) (ROI)، وقياس أثر المساهمة في زيادة الكفاءة المالية والتشغيلية.
2. اعتماد الإطار العام لإدارة وضبط ومراقبة موارد ومشاريع تكنولوجيا المعلومات يحاكي أفضل الممارسات الدولية المقبولة بهذا الخصوص وعلى وجه التحديد COBIT يتوافق ويلبي تحقيق أهداف ومتطلبات التعليمات من خلال تحقيق الأهداف المؤسسية بشكل مستدام، وتحقيق مصفوفة Alignment Goals المصاحبة لها والواردة في الاطار المرجعي COBIT 2019 ويغطي اهداف الحاكمية والادارة الواردة في الاطار المرجعيCOBIT 2019.
3. اعتماد مصفوفة الأهداف المؤسسية الواردة في الاطار المرجعي COBIT 2019، وAlignment Goals المصاحبة لها واعتبار معطياتها حداً أدنى، وتوصيف الأهداف الفرعية اللازمة لتحقيقها.
4. اعتماد مصفوفة للمسؤوليات (RACI Chart) تجاه الأهداف الرئيسية لحاكمية تكنولوجيا المعلومات في الاطار المرجعي COBIT 2019 والعمليات الفرعية المنبثقة عنها من حيث: الجهة أو الجهات أو الشخص أو الأطراف المسؤولة بشكل أولي (Responsible)، وتلك المسؤولة بشكل نهائي (Accountable)، وتلك الجهه المستشارة (Consulted)، وتلك التي يتم إطلاعها (Informed) على كافة الاهداف المختاره ضمن نظام حاكمية المعلومات والتكنولوجيا المصاحبه لها في البنك، مسترشدين بمعيار COBIT 2019.

5. التأكد من وجود إطار عام لإدارة مخاطر تكنولوجيا المعلومات يتوافق ويتكامل مع الإطار العام الكلي لإدارة المخاطر في البنك وبحيث يأخذ بعين الاعتبار ويلبي كافة اهداف حاكمية وإدارة تكنولوجيا المعلومات الواردة في الاطار المرجعي COBIT 2019.
6. اعتماد موازنة موارد ومشاريع تكنولوجيا المعلومات بما يتوافق والأهداف الاستراتيجية للبنك.
7. الاشراف العام والاطلاع على سير عمليات وموارد ومشاريع تكنولوجيا المعلومات للتأكد من كفايتها ومساهمتها الفاعلة في تحقيق متطلبات وأعمال البنك.
8. الإطلاع على تقارير التدقيق لتكنولوجيا المعلومات واتخاذ ما يلزم من إجراءات لمعالجة الإنحرافات.
9. التوصية للمجلس باتخاذ الإجراءات اللازمة لتصحيح أية إنحرافات.
10. تتولى لجنة الحاكمية لتكنولوجيا المعلومات بالإضافة الى مهامها اعتماد أهمية وترتيب أولوية الأهداف الواردة في الاطار المرجعي COBIT 2019 (Governance & Management Objectives) ومدى ارتباطها مع الأهداف المؤسسية و Alignment Objectives بالإضافة الى مكونات نظام الحاكمية الستة وذلك بناءا على دراسة نوعية و/او كمية تعد لهذا الغرض بشكل سنوي على الأقل وتأخذ بالاعتبار Design Factors الواردة في COBIT 2019 – Design Guide.

ب. اللجنة التوجيهية لتكنولوجيا المعلومات:

- يتم تشكيل اللجنة برئاسة الرئيس التنفيذي وعضوية مدراء الادارة التنفيذية العليا بما في ذلك مدير تكنولوجيا المعلومات ومدير إدارة المخاطر ومدير أمن المعلومات، وينتخب المجلس احد اعضائه ليكون عضواً مراقباً في هذه اللجنة بالإضافة للمدقق العام.
- يمكنها دعوة الغير لدى الحاجة لحضور اجتماعاتها.
- توثق اللجنة اجتماعاتها بمحاضر اصولية.
- تكون دورية الاجتماعات مرة كل ثلاثة اشهر على الاقل.
- تتولى اللجنة – كحد أدنى – المهام التالية:

1. وضع الخطط السنوية الكفيلة بالوصول للأهداف الاستراتيجية المقرة من قبل المجلس، والإشراف على تنفيذها لضمان تحقيقها ومراقبة العوامل الداخلية والخارجية المؤثرة عليها بشكل مستمر.
2. ربط مصفوفة الأهداف المؤسسية بمصفوفة Alignment Goals المصاحبة لها وكما وردت في الاطار المرجعي COBIT 2019 واعتمادها ومراجعتها بشكل مستمر وبما يضمن تحقيق الأهداف

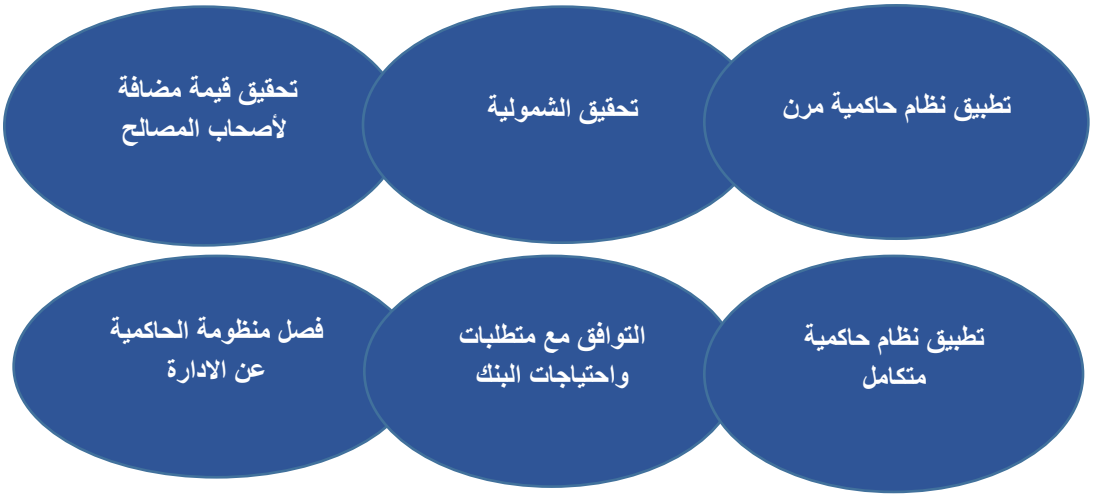
الاستراتيجية للبنك وأهداف التعليمات، ومراعاة تعريف مجموعة معايير للقياس ومراجعتها وتكليف المعنيين من الإدارة التنفيذية بمراقبتها بشكل مستمر وإطلاع اللجنة على ذلك.

3. دعم تحقيق الأهداف وعمليات حاكمية تكنولوجيا المعلومات (Alignment Goals, and Governance and Management Objectives) كحد أدنى من خلال التوصية بتخصيص الموارد المالية وغير المالية اللازمة لتحقيق Alignment Goals واهداف حاكمية تكنولوجيا المعلومات الواردة في الاطار المرجعي COBIT 2019، 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 الأخرى المتعلقة بها خدمة للأهداف، وتولي عمليات الإشراف على سير تنفيذ مشاريع وعمليات حاكمية تكنولوجيا المعلومات.
4. المراجعة المستمرة لمشاريع وبرامج تكنولوجيا المعلومات وترتيبها من حيث الأولوية والمخاطره.
5. التأكد من تنفيذ المشاريع والتناسق مابين المشاريع ومتطلبات مراكز الاعمال.
6. متابعة المشاريع وحالات الشراء والاحالة والتعديلات المتعلقه بأنظمة المعلومات والتكنولوجيا المصاحبة لها وتقديم التوصيات المناسبة بخصوصها.
7. مراقبة مستوى الخدمات الفنية والتكنولوجية والعمل على رفع كفاءتها وتحسينها بشكل مستمر.
8. تقييم ومراجعة ميزانية الأنظمة السنوية (الرأسمالية والتشغيلية) واستراتيجية الأنظمة لضمان توافقها المستمر مع إستراتيجية الأعمال ومتطلبات الجهات الرقابية بشكل نصف سنوي وتقييم المنجزات خلال هذه الفترة، والتوصية بإتخاذ الإجراءات التصحيحية المناسبة.
9. رفع التوصيات اللازمة للجنة حاكمية تكنولوجيا المعلومات بخصوص الأمور التالية:
    - تخصيص الموارد اللازمة والآليات الكفيلة بتحقيق مهام لجنة حاكمية تكنولوجيا المعلومات.
    - أية إنحرافات قد تؤثر سلبا على تحقيق الأهداف الاستراتيجية.
    - أية مخاطر غير مقبولة متعلقة بتكنولوجيا وأمن وحماية المعلومات.
    - تقارير الأداء والامتثال بمتطلبات الإطار العام لإدارة وضبط ومراقبة موارد ومشاريع تكنولوجيا المعلومات
    - تقارير خاصة بأبرز المخاطر المتعلقة بتكنولوجيا المعلومات والناتجة عن عمليات تحليل المخاطر.
10. تزويد لجنة حاكمية تكنولوجيا المعلومات بمحاضر اجتماعاتها أولا بأول والحصول على ما يفيد الاطلاع عليها.

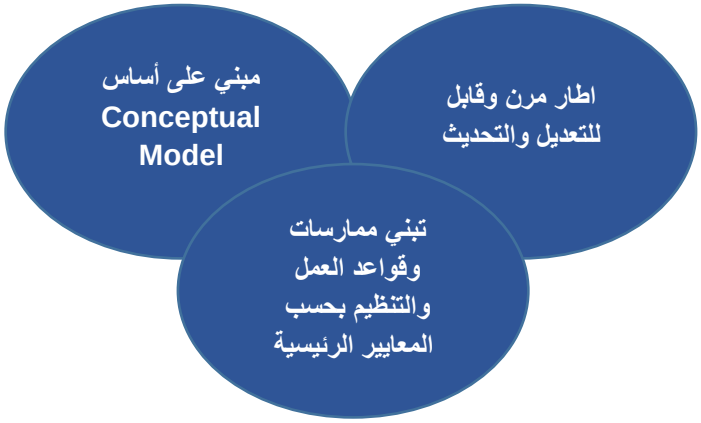
سادساً: مبادئ اطار حاكمية تكنولوجيا المعلومات

تنقسم مبادئ حاكمية تكنولوجيا المعلومات الى مجموعتين:

المجموعة الأولى: وهي المبادئ الأساسية والجوهرية التي تشكل نظام الحاكمية Governance System



المجموعة الثانية: المبادئ المرتبطة باطار الحاكمية Governance Framework اللازمة لبناء نظام الحاكمية على مستوى البنك.



سابعا: أهداف حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها:

أ. تلبية احتياجات أصحاب المصالح (Stakeholder's Needs) وتحقيق توجهات وأهداف البنك من خلال تحقيق أهداف المعلومات والتكنولوجيا المصاحبة لها، وبما يضمن:

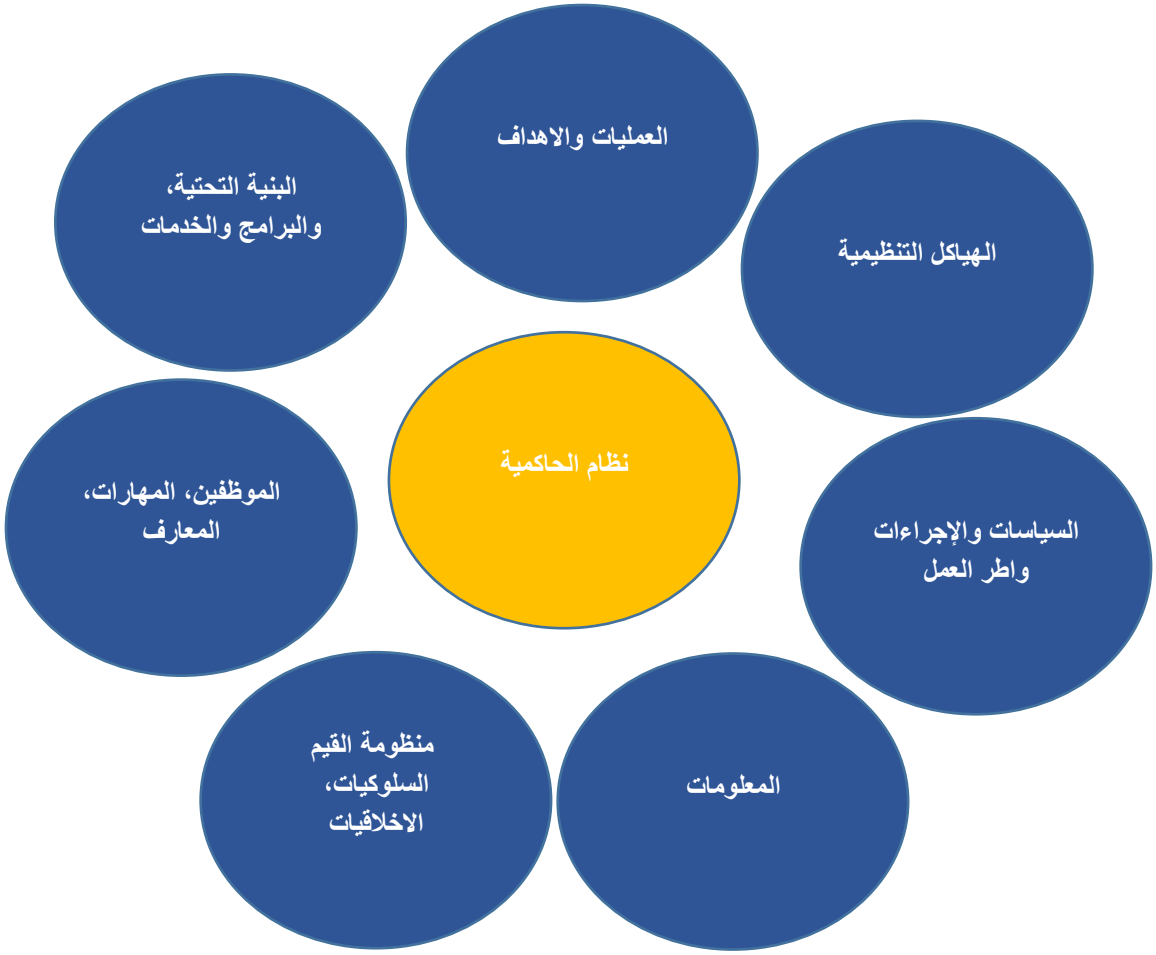
1. توفير معلومات ذات جودة عالية كمرتكز يدعم آليات صنع القرار في البنك.
2. إدارة حصيفة لموارد ومشاريع تكنولوجيا المعلومات، تعظم الاستفادة من تلك الموارد وتقلل الهدر منها.
3. توفير بنية تحتية تكنولوجية متميزة وداعمه تمكن البنك من تحقيق أهدافه.
4. الإرتقاء بعمليات البنك المختلفة من خلال توظيف منظومة تكنولوجية كفؤة وذات اعتمادية متميزة.
5. إدارة حصيفة لمخاطر تكنولوجيا المعلومات تكفل الحماية اللازمة لموجودات البنك.
6. المساعدة في تحقيق الامتثال لمتطلبات القوانين والتشريعات والتعليمات بالإضافة للامتثال لاستراتيجية وسياسات وإجراءات العمل الداخلية.
7. تحسين نظام الضبط والرقابة الداخلي.
8. تعظيم مستوى الرضا عن تكنولوجيا المعلومات من قبل مستخدميها بتلبية احتياجات العمل بكفاءة وفعالية.
9. إدارة خدمات الأطراف الخارجية الموكل إليها تنفيذ عمليات ومهام وخدمات ومنتجات.

ب. تبني ممارسات وقواعد العمل والتنظيم بحسب أفضل المعايير الدولية كنقطة انطلاق يتم الارتكاز والبناء عليها في مجالي حاكمية وإدارة عمليات ومشاريع وموارد تكنولوجيا المعلومات.

ج. فصل عمليات ومهام ومسؤوليات المجلس في مجال الحاكمية عن تلك التي تقع ضمن حدود مسؤولية الإدارة التنفيذية بخصوص المعلومات والتكنولوجيا المصاحبة لها.

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

ثامنا: مكونات نظام الحاكمية Governance System Components



1. السياسات والإجراءات واطر العمل

- على المجلس أو من يفُوضّ من لجانه اعتماد منظومة المبادئ والسياسات وأطر العمل (Frameworks) اللازمة لتحقيق الإطار العام لإدارة وضبط ومراقبة موارد ومشاريع تكنولوجيا المعلومات وبما يلبي متطلبات الأهداف وعمليات حاكمية تكنولوجيا المعلومات الواردة في الاطار المرجعي COBIT 2019
- على المجلس أو من يفُوضّ من لجانه اعتماد المبادئ والسياسات وأطر العمل وعلى وجه الخصوص تلك المتعلقة بإدارة مخاطر تكنولوجيا المعلومات، وإدارة أمن المعلومات، وإدارة الموارد البشرية والتي تلبي متطلبات واهداف وعمليات حاكمية تكنولوجيا المعلومات الواردة في. الاطار المرجعيCOBIT 2019
- على المجلس أو من يفُوضّ من لجانه اعتماد منظومة السياسات اللازمة لإدارة موارد وعمليات حاكمية تكنولوجيا المعلومات والواردة بالمرفق رقم 6 من التعليمات واعتبار منظومة السياسات هذه حدا أدنى مع إمكانية الجمع والدمج لتلك السياسات حسب ما تقتضيه طبيعة العمل، وعلى أن يتم تطوير سياسات أخرى ناظمة مواكبة لتطور أهداف البنك وآليات العمل، وعلى أن تحدد كل سياسة الجهة المالكة ونطاق التطبيق ودورية المراجعة والتحديث وصلاحيات الاطلاع والتوزيع والأهداف والمسؤوليات وإجراءات العمل المتعلقة بها والعقوبات في حال عدم الامتثال وآليات فحص الامتثال.
- يراعى لدى انشاء السياسات مساهمة كافة الشركاء الداخليين والخارجيين واعتماد أفضل الممارسات الدولية وتحديثاتها كمراجع لصياغة تلك السياسات مثل COBIT 2019 ,COBIT5, ISO/IEC 27001/2, ISO 31000, ISO/IEC 38500, ISO/IEC 9126, ISO/IEC 15504, ISO 22301, PCI. DSS, ITIL…etc.

2. الأهداف وعمليات حاكمية تكنولوجيا المعلومات

- قيام البنك بإعداد واعتماد مصفوفة للمسؤوليات والمعلومات RACI حسب الأهداف والعمليات الواردة في الاطار المرجعي COBIT 2019 من حيث: الجهة أو الجهات وتلك المسؤولة بشكل اولي Responsible وتلك المسؤولة بشكل نهائي Accountable وتلك المستشارة Consulted وتلك التي يتم إطلاعها Informed تجاه كافة العمليات في المرفق المذكور مسترشدين بالاطار المرجعي COBIT 2019 واعتمادها من قبل اللجان المشار اليها في التعليمات.
- قيام البنك بإعداد إطار عام لإدارة مخاطر تكنولوجيا المعلومات يتوافق ويتكامل مع الإطار العام الكلي لإدارة المخاطر في البنك وبحيث يأخذ بعين الاعتبار ويلبي كافة اهداف حاكمية تكنولوجيا المعلومات الواردة في الاطار المرجعي COBIT 2019.
- قيام البنك بتوفير الوسائل لتحقيق Alignment Goals واهداف حاكمية تكنولوجيا المعلومات الواردة في الاطار المرجعي COBIT 2019

- تعتبر Alignment Goals واهداف حاكمية تكنولوجيا المعلومات الواردة في الاطار المرجعي COBIT 2019 ومعطياتها حدا أدنى يتوجب على إدارة البنك العليا الامتثال لها وتحقيقها بشكل مستمر، وتعتبر اللجنة التوجيهية لتكنولوجيا المعلومات المسؤول الأول عن ضمان الامتثال بتحقيق متطلباتها، ولجنة حاكمية تكنولوجيا المعلومات والمجلس ككل المسؤول النهائي بهذا الخصوص ويتوجب على كافة دوائر البنك وعلى وجه الخصوص دائرة تكنولوجيا المعلومات وإدارة أمن المعلومات وإدارة المشاريع تحديد عملياتها وإعادة صياغتها بحيث تحاكي وتغطي متطلبات كافة اهداف حاكمية تكنولوجيا المعلومات الواردة في الاطار المرجعي COBIT 2019
- التأكّد من توافق اهداف حاكمية تكنولوجيا المعلومات الواردة الاطار المرجعي COBIT 2019 مع Alignment Goals والمساهمة في تحقيقيها والتوافق وتحقيق الأهداف المؤسسية الواردة في الاطار المرجعي COBIT
- يتولى المجلس المسؤولية المباشرة لعمليات التقييم والتوجيه والرقابة EDM – Evaluate, Direct & Monitor وحسب الاطار المرجعي COBIT 2019
- يتولى المجلس ودائرة ادارة المخاطر المسؤولية المباشرة عن عمليّة ضمان إدارة حصيفة لمخاطر تكنولوجيا المعلومات EDM03 (Ensured Risk optimization) وعملية ادارة المخاطر APO12 (Managed Risk)

3. الهياكل التنظيمية

- على المجلس اعتماد الهياكل التنظيمية (الهرمية واللجان) وعلى وجه الخصوص تلك المتعلقة بإدارة موارد وعمليات ومشاريع تكنولوجيا المعلومات، وإدارة مخاطر تكنولوجيا المعلومات، وإدارة أمن المعلومات، وإدارة الموارد البشرية والتي تلبي متطلبات اهداف حاكمية تكنولوجيا المعلومات الواردة في الاطار المرجعي COBIT 2019 وتحقيق أهداف البنك 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 للبنك.

4. المعلومات والتقارير

- على المجلس والإدارة التنفيذية العليا تطوير البنية التحتية ونظم المعلومات اللازمة لتوفير المعلومات والتقارير لمستخدميها كمرتكز لعمليات اتخاذ القرار في البنك، وعليه يجب أن 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 الأخرى الواردة في COBIT 2019.

- على المجلس أو من يفُوضّ من لجانه اعتماد منظومة المعلومات والتقارير الواردة في المرفق رقم 7 من التعليمات واعتبار تلك المنظومة حداً أدنى، مع مراعاة تحديد مالكين لتلك المعلومات والتقارير تحدد من خلالهم وتفوض صلاحيات الاطلاع والاستخدام بحسب الحاجة للعمل والشركاء المعنيين، وعلى أن يتم مراجعتها وتطويرها بشكل مستمر لمواكبة تطور أهداف وعمليات البنك وبما يتفق وأفضل الممارسات الدولية المقبولة بهذا الخصوص.

5. الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات

- على المجلس أو من يفُوضّ من لجانه والإدارة التنفيذية العليا اعتماد منظومة الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات الداعمة والمساعدة لتحقيق عمليات حاكمية تكنولوجيا المعلومات وبالتالي أهداف المعلومات والتكنولوجيا المصاحبة لها، وبالتالي الأهداف المؤسسية.
- على المجلس أو من يفُوضّ من لجانه والإدارة التنفيذية العليا اعتماد منظومة الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات الواردة في المرفق رقم 8 من التعليمات، واعتبار تلك المنظومة حدا أدنى، وعلى أن يتم توفيرها وتطويرها بشكل مستمر لمواكبة تطور أهداف وعمليات البنك وبما يتفق وأفضل الممارسات الدولية المقبولة بهذا الخصوص.

6. المعارف والمهارات والخبرات

- على المجلس أو من يفُوضّ من لجانه اعتماد مصفوفة المؤهلات HR Competencies وسياسات إدارة الموارد البشرية اللازمة لتحقيق متطلبات عمليات حاكمية تكنولوجيا المعلومات الواردة في المرفق رقم 3 من التعليمات ومتطلبات التعليمات بشكل عام، وضمان وضع الشخص المناسب في المكان المناسب.
- على إدارة البنك توظيف العنصر البشري المؤهل والمدرب من الأشخاص ذوي الخبرة في مجالات إدارة موارد تكنولوجيا المعلومات وإدارة المخاطر وإدارة أمن المعلومات وإدارة تدقيق تكنولوجيا المعلومات اعتمادا على معايير المعرفة الأكاديمية والمهنية والخبرة العملية باعتراف جمعيات دولية مؤهلة بموجب معايير الاعتماد الدولي للمؤسسات المانحة للشهادات المهنية (ISO/IEC 17024) و Skills Framework for Information Age SFIA و/أو أية معايير أخرى موازية كل بحسب اختصاصه، على أن يتم إعادة تأهيل وتدريب الكوادر الموظفة. بشكل مستمر لتلبية المتطلبات الداخليه والخارجيه.
- على الإدارة التنفيذية في البنك الاستمرار برفد موظفيها ببرامج التدريب والتعليم المستمر للحفاظ على مستوى من المعارف والمهارات يلبي ويحقق اهداف حاكمية تكنولوجيا المعلومات الواردة في الاطار المرجعي COBIT 2019.
- على الإدارة التنفيذية في البنك تضمين آليات التقييم السنوي Performance Evaluation للكوادر بمعايير قياس موضوعية تأخذ بعين الاعتبار المساهمة من خلال المركز الوظيفي بتحقيق أهداف البنك.

7. منظومة القيم والأخلاق والسلوكيات

- على المجلس أو من يفُوضّ من لجانه اعتماد منظومة أخلاقية مهنية مؤسسية تعكس القواعد السلوكية المهنية الدولية المقبولة بخصوص التعامل مع المعلومات والتكنولوجيا المصاحبة لها تحدد بوضوح القواعد السلوكية المرغوبة وغير المرغوبة وتبعاتها.
- على المدقق الداخلي والمدقق الخارجي الامتثال لمنظومة الأخلاق والممارسات المهنية المعتمدة من قبل المجلس بحيث تتضمن بالحد الأدنى منظومة الأخلاق المهنية الواردة في المعيار الدولي (ITAF) (Information Technology Assurance Framework) الصادر عن جمعية التدقيق والرقابة على نظم المعلومات وتحديثاته (ISACA) .
- على المجلس والإدارة التنفيذية العليا توظيف الآليات المختلفة لتشجيع تطبيق السلوكيات المرغوبة وتجنب السلوكيات غير المرغوبة من خلال اتباع أساليب الحوافز والعقوبات على سبيل المثال لا الحصر.

تاسعا: الأهداف ذات الأولوية والاهمية العليا Focus Area

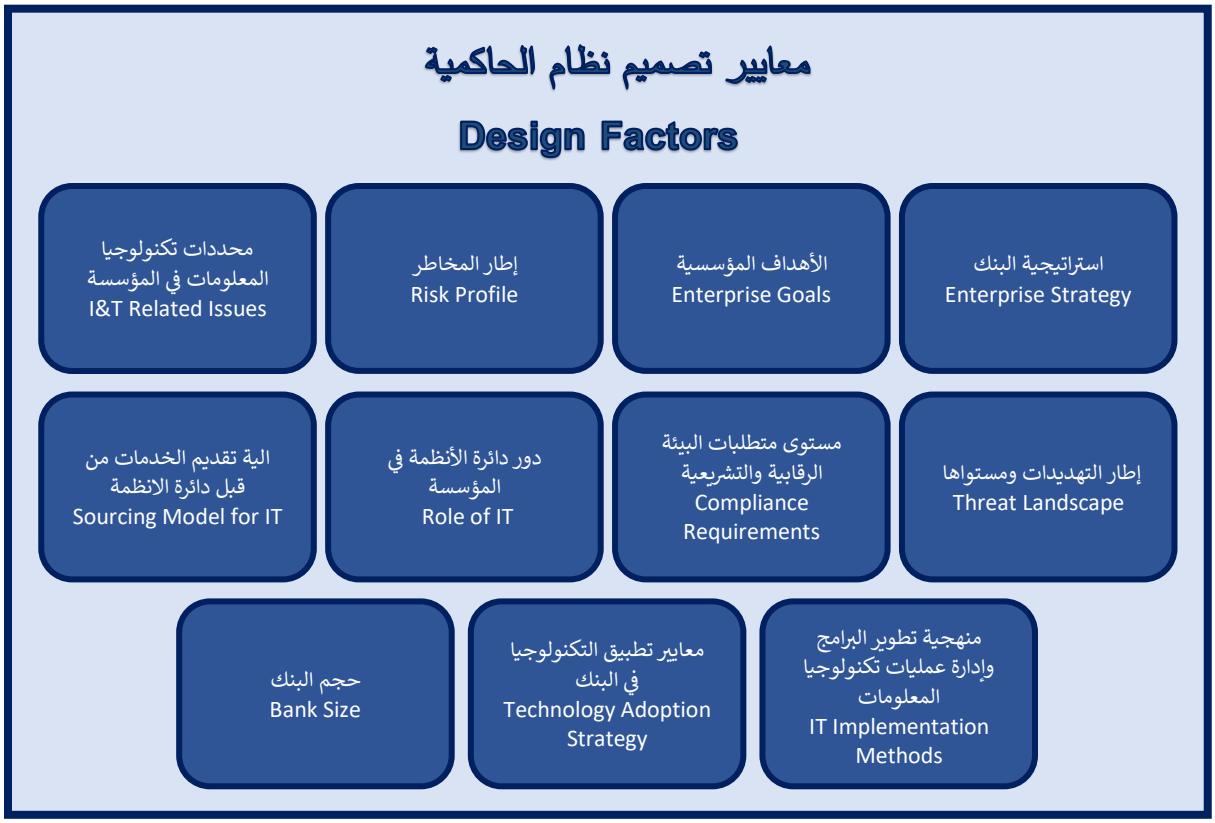
تعتبر اهداف الحاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها بالإضافة الى مكونات نظام الحاكمية والمرتبطة بنشاطات ومواضيع (الامن السيبراني، إدارة المخاطر، وخصوصية وحماية البيانات، والامتثال، والمراقبة، التدقيق والتوافق الاستراتيجي عبارة عن (Focus Area) ذات أهمية وأولوية عليا.

عاشرا: معايير تصميم نظام الحاكمية Design Factor

يتم تصميم نظام حاكمية وادارة المعلومات والتكنولوجيا المصاحبه لها بالاعتماد على منهجيه التصميم الموصى بها في الاطار المرجعي "COBIT 2019 Design Guide"، حيث يتم الاخذ بعين الاعتبار جميع او بعض من معايير التصميم المذكوره ادناه، من خلال اعطاء وزن لكل خاصيه أو محور كما هو مذكور في الجدول ادناه وبما يتناسب وتقييم وضع البنك واستراتيجيته الحاليه:

الرقم	المعيار	خصائص/محاور المعيار
.1	استراتيجية البنك	- استراتيجية النمو وزيادة الأرباح - استراتيجية الابداع والتميز - استراتيجية تخفيض النفقات والكلف التشغيلية - استراتيجية خدمة العملاء
.2	الأهداف المؤسسية	يتم اعطاء وزن لكل من أهداف المؤسسة المذكوره ضمن إطار COBIT2019 وبما يتناسب مع اهداف البنك الاستراتيجيه.

.3	اطار المخاطر	يتم تحديد الأثر واحتمالية حدوث كل من المخاطر المذكوره ضمن إطار COBIT2019، وبما يتناسب مع سجل المخاطر لأنظمة المعلومات والتكنولوجيا المصاحبه لها.
.4	محددات تكنولوجيا المعلومات في المؤسسة	يتم تحديد اهم الصعوبات التي تواجه دائرة انظمة المعلومات والتكنولوجيا من خلال قائمة التحديات والصعوبات المذكوره في دليل إطار COBIT2019.
.5	إطار التهديدات ومستواها	– حجم التهديدات التي من الممكن ان يتعرض لها البنك (معتدل) – حجم التهديدات التي من الممكن ان يتعرض لها البنك (مرتفع)
.6	مستوى متطلبات البيئة الرقابية والتشريعية	– محدودة – متوسط – مرتفعة
.7	دور دائرة الأنظمة في المؤسسة	– يدعم ويخدم البنك ولا يعتبر مؤثر بشكل مباشر على استمرارية الاعمال – يدعم ويخدم البنك ويؤثر بشكل مباشر على استمرارية الاعمال – دور تطوري وابداعي ولا يؤثر على استمرارية اعمال البنك – دور استراتيجي وداعم لخطط وتطور الاعمال ويؤثر بشكل جوهري على البنك
.8	الية تقديم الخدمات من قبل دائرة الانظمة	– من خلال الاسناد الخارجي – من خلال الموارد الداخلية – من خلال السحابة المحوسبة – من خلال أنماط متعددة تشمل الموارد المحلية والاسناد الخارجي والسحابة المحوسبة
.9	منهجية تطوير البرامج وإدارة عمليات تكنولوجيا المعلومات	– منهجية Agile – منهجية DevOps – المفهوم التقليدي (Waterfall) – خليط من الأنماط أعلاه.
10	معايير تطبيق التكنولوجيا في البنك.	– مبادر وسباق في تطبيق أفضل المعايير التكنولوجية. – مبادر في تطبيق أفضل المعايير التكنولوجية بعد نضوجها وتطبيقها في بنوك اخرى. – غير مبادر وغير سباق في تطبيق أفضل المعايير التكنولوجية ويأخذ وقت لاعتمادها.
11	حجم البنك	– كبير من حيث عدد الموظفين (أكثر من 250 موظف) – متوسط/صغير (اقل من 250 موظف)



- يعتمد البنك منهجية Goals Cascade للوصول الى إطار حاكمية مؤسسي بالاعتماد على ما يلي:

احدى عشر: التدقيق الداخلي والخارجي:

1. على المجلس رصد الموازنات الكافية وتخصيص الأدوات والموارد اللازمة بما في ذلك العنصر البشري المؤهل من خلال فريق متخصص بالتدقيق على تكنولوجيا المعلومات، والتأكد من أن كل من دائرة التدقيق الداخلي في البنك والمدقق الخارجي قادرين على مراجعة وتدقيق عمليات توظيف وإدارة موارد ومشاريع تكنولوجيا المعلومات وعمليات البنك المرتكزة عليها مراجعة فنية متخصصة (IT Audit) بحسب البند 4 أدناه، من خلال كوادر مهنية مؤهلة ومعتمدة دوليا بهذا المجال، حاصلين على شهادات اعتماد مهنية سارية مثل (CISA) من جمعيات دولية مؤهلة بموجب معايير الاعتماد الدولي للمؤسسات المانحة للشهادات المهنية (ISO/IEC17024) و/أو أية معايير اخرى موازية.
2. على لجنة التدقيق المنبثقة عن المجلس من جهة والمدقق الخارجي من جهة أخرى تزويد البنك المركزي الأردني بتقرير سنوي للتدقيق الداخلي وآخر للتدقيق الخارجي على التوالي يتضمن رد الإدارة التنفيذية وإطلاع وتوصيات المجلس بخصوصه، وذلك بحسب ما ورد في البند 4.2 أدناه ووفق نموذج تقرير تدقيق (مخاطر–ضوابط) المعلومات والتكنولوجيا المصاحبة لها في المرفق رقم 4 من التعليمات، وذلك خلال الربع الأول من كل عام، وتحل هذه التقارير محل نظيرتها أو التي تشملها من التقارير المطلوبة بموجب تعليمات سابقة.
3. على لجنة التدقيق تضمين مسؤوليات وصلاحيات ونطاق عمل تدقيق تكنولوجيا المعلومات ضمن ميثاق التدقيق (Audit Charter) من جهة وضمن إجراءات متفق عليها مع المدقق الخارجي من جهة أخرى، وبما يتوافق ويغطي التعليمات.
4. على المجلس التأكد ومن خلال لجنة التدقيق المنبثقة عنه من قيام المدقق الداخلي والمدقق الخارجي للبنك لدى تنفيذ عمليات التدقيق المتخصص للمعلومات والتكنولوجيا المصاحبة لها الإلتزام بما يلي:

4.1. معايير تدقيق تكنولوجيا المعلومات بحسب آخر تحديث للمعيار الدولي ITAF Information Technology Assurance Framework الصادر عن جمعية التدقيق والرقابة على نظم المعلومات ISACA ومنها:

- تنفيذ مهمات التدقيق ضمن خطة معتمدة بهذا الخصوص تأخذ بعين الاعتبار الأهمية النسبية للعمليات ومستوى المخاطر ودرجة التأثير على أهداف ومصالح البنك.
- توفير والإلتزام بخطط التدريب والتعليم المستمر من قبل الكادر المتخصص بهذا الصدد.
- الإلتزام بمعايير الاستقلالية المهنية والإدارية Professional and Organizational Independency وضمان عدم تضارب المصالح الحالية والمستقبلية.
- الإلتزام بمعايير الموضوعية (Objectivity) وبذل العناية المهنية Due Professional Care والحفاظ المستمر على مستوى التنافسية والمهنية (Proficiency) من المعارف والمهارات الواجب

التمتع بها، ومعرفة عميقة في آليات وعمليات البنك المختلفة المرتكزة على تكنولوجيا المعلومات وتقارير المراجعة والتدقيق الأخرى (المالية والتشغيلية والقانونية)، والقدرة على تقديم الدليل (Evidence) المتناسب مع الحالة، والحس العام في كشف الممارسات غير المقبولة والمخالفة لأحكام القوانين والأنظمة والتعليمات.

4.2. فحص وتقييم ومراجعة عمليات توظيف وإدارة موارد تكنولوجيا المعلومات وعمليات البنك المرتكزة عليها وإعطاء رأي عام (Reasonable Overall Audit Assurance) حيال مستوى المخاطر الكلي للمعلومات والتكنولوجيا المصاحبة لها ضمن برنامج تدقيق يشمل على الأقل المحاور المبينة في المرفق رقم 5 من التعليمات، على أن يكون تكرار التدقيق لكافة المحاور أو جزء منها كحد أدنى مرة واحدة سنويا على الأقل في حال تم تقييم المخاطر بدرجة 4 او 5 بحسب سلم تقييم المخاطر الموضح في المرفق رقم 4 من التعليمات، ومرة واحدة كل سنتين على الأقل في حال تم تقييم المخاطر بدرجة 3، ومرة واحدة كل ثلاث سنوات على الأقل في حال تم تقييم المخاطر بدرجة 2 او 1، مع مراعاة التغير المستمر في مستوى المخاطر والأخذ بعين الاعتبار التغيرات الجوهرية التي تطرأ على بيئة المعلومات والتكنولوجيا المصاحبة لها خلال فترات التدقيق المذكورة، على أن يتم تزويد البنك المركزي بتقارير التدقيق لأول مرة بغض النظر عن درجة تقييم المخاطر، وعلى أن تشمل عمليات التقييم للمحاور المذكورة آليات البنك المتبعة من حيث التخطيط الاستراتيجي ورسم السياسات والمبادئ وإجراءات 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 أهمية الاختلالات ونقاط الضعف (الملاحظات) بالإضافة للضوابط المفعلة وتقييم مستوى المخاطر المتبقية والمتعلقة بكل منها باستخدام معيار منهجي لتحليل وقياس المخاطر، متضمنا الإجراءات التصحيحية المتفق عليها والمنوي اتباعها من قبل إدارة البنك بتواريخ محددة للتصحيح، مع الإشارة ضمن جدول خاص إلى الرتبة الوظيفية لصاحب المسؤولية في البنك مالك كل ملاحظة.

4.3. إجراءات منتظمة لمتابعة نتائج التدقيق للتأكد من معالجة الملاحظات والاختلالات الواردة في تقارير المدقق بالمواعيد المحددة، والعمل على رفع مستوى الأهمية والمخاطر تصعيدا تدريجيا في حال عدم الاستجابة ووضع المجلس بصورة ذلك كلما تطلب الأمر.

4.4. تضمين آليات التقييم السنوي (Performance Evaluation) لكوادر تدقيق تكنولوجيا المعلومات بمعايير قياس موضوعية تأخذ كل ما ورد في البند 4 أعلاه بعين الاعتبار، وعلى أن تتم عمليات التقييم من قبل المجلس ممثلا بلجنة التدقيق المنبثقة عنه.

5. من الممكن إسناد (Outsource) دور المدقق الداخلي للمعلومات والتكنولوجيا المصاحبة لها (Internal IT Audit) لجهة خارجية متخصصة مستقلة تماما عن المدقق الخارجي المعتمد بهذا الخصوص، شريطة

تلبية كافة متطلبات التعليمات وأية تعليمات أخرى ذات صلة واحتفاظ لجنة التدقيق المنبثقة عن المجلس والمجلس نفسه بدورهما فيما يتعلق بفحص الامتثال والتأكد من تلبية هذه المتطلبات كحد أدنى.

6. يسمح باعتماد تقارير المدقق الداخلي والخارجي من قبل لجنة حاكمية تكنولوجيا المعلومات او اللجنة القائمة مقامها على ان يتم اطلاع المجلس على تلك التقارير.

اثنى عشر: نطاق وآلية تطبيق وتبني نظام حاكمية وادارة المعلومات والتكنولوجيا المصاحبه لها ومهام الأطراف الرئيسيه:

أولاً: نطاق وآلية تطبيق وتبني نظام حاكمية وادارة المعلومات والتكنولوجيا المصاحبه لها:

- يشمل نطاق تطبيق التعليمات كافة عمليات البنك المرتكزة على تكنولوجيا المعلومات بمختلف الفروع والدوائر، وتعتبر جميع الأطراف أصحاب المصالح معنية بتطبيق التعليمات كل بحسب دوره وموقعه.
- تعتبر الاهدف الواردة في الاطار المرجعي COBIT 2019 وباقي عناصر التمكين السته المرتبطة بنشاطات تتعلق بمواضيع الامن السيبراني وإدارة المخاطر وخصوصية وحماية البيانات والامتثال والمراقبة والتدقيق والتوافق الاستراتيجي عبارة عن Focus Areas ذات أهمية واولوية عليا.
- يجب ان يتناسب مستوى نضوج (Capability Level) النشاطات المتعلقة بالأهداف الواردة في الإطار المرجعي COBIT 2019 وعناصر التمكين المرتبطة بها بشكل طردي مع درجة الأهمية والاولية بحسب نتائج الدراسة التي تجريها لجنة حاكمية تكنولوجيا المعلومات والمشار اليها أعلاه، على ان لا يقل مستوى النضوج للنشاطات المتعلقة بالاهداف ذات الأهمية والاولوية العليا عن المستوى (3) (Fully Achieved) بحسب سلم النضوج الوارد في الاطار COBIT 2019، ويسمح باعتبار ما لايزيد عن 26% من الأهداف الواردة في الاطار COBIT 2019 ضمن اهداف الإدارة العليا (بما لايزيد عن 9 اهداف بحد اقصى من اصل 35 هدف) على انها اهداف ذات أهمية واولوية ادنى اعتماد على نتائج دراسة نظام حاكمية وادارة المعلومات والتكنولوجيا المصاحبه لها والمعتمده من لجنة حاكمية المعلومات.
- على البنك عند توقيع اتفاقيات إسناد (Outsourcing) مع الغير لتوفير الموارد البشرية والخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات بهدف تسيير عمليات البنك التأكد من إلتزام الغير بتطبيق بنود هذه التعليمات بشكل كلي أو جزئي بالقدر الذي يتناسب مع أهمية وطبيعة عمليات البنك والخدمات والبرامج والبنية التحتية المقدمة قبل وأثناء فترة التعاقد، وبما لا يعفي المجلس والإدارة التنفيذية العليا من المسؤولية النهائية لتحقيق متطلبات التعليمات بما في ذلك متطلبات التدقيق الواردة في الدليل.
- يتوجب على البنك مواكبة الإصدارات الناشئة المستقبلية وتحديثاتها فيما يخص الإطار العام COBIT وما يحتويه من معايير دولية أخرى مستند لها ضمن هذا الإطار.

- لا بد عند التطبيق والدخول في تفاصيل الدعامات (الممكنات) السبعة والمرفقات والعمليات والأهداف الفرعية أن تقوم البنوك بتطويع (Tailoring) وبما ينسجم ومعطيات البنك لخدمة أهداف ومتطلبات التعليمات والمعيار COBIT2019 والعمل على إيجاد التغيير المطلوب لتوفير وتهيئة البيئة اللازمة للتطبيق.
- يقوم البنك باتباع أسلوب تحليل الإنحراف Gap Analysis بين الوضع الحالي والمقارنة مع متطلبات التعليمات والمعيار تمهيدا لعملية التطبيق اخذين بالاعتبار الأهداف التي يسعى البنك لتحقيقها، الوضع الحالي، الوضع المستقبلي.
- على البنك إرسال تقرير الإنجاز المتعلق بالامتثال لتحقيق متطلبات التعليمات البنك المركزي الاردني كل ستة أشهر من تاريخ التعليمات، موضحا فيه مستوى الإنجاز لكل بند من بنود التعليمات حسب تعاميم وتعليمات البنك المركزي.

ثانياً: الأطراف الرئيسيه ومهامها:

- **رئيس وأعضاء المجلس والخبراء الخارجيين المستعان بهم:** تولي مسؤوليات التوجيه العام لتبني والحفاظ على حاكمية وادارة المعلومات والتكنولوجيا المصاحبه لها بالمستويات المحدده والموافقة على المهام والمسؤوليات، والدعم وتقديم التمويل اللازم.
- **الرئيس التنفيذي ونوابه ومساعديه ورؤساء المجموعات ومسؤولي العمليات ومدراء الفروع:** تولي مسؤوليات تسمية الأشخاص المناسبين من ذوي الخبرة لتمثيلهم في مشاريع وادارة عمليات المعلومات والتكنولوجيا المصاحبه لها وتوصيف مهامهم ومسؤولياتهم.
- **لجنة حاكمية تكنولوجيا المعلومات واللجنه التوجيهيه لتكنولوجيا المعلومات:** تولي المسؤوليات المنوطه بموجب المهام الموضحه ضمن البند الخامس من هذا الدليل (صفحه 5).
- **التدقيق الداخلي:** تولي مسؤولياته المنوطة به بموجب التعليمات بشكل مباشر، والمشاركة في تبني وتطبيق النظام بما يمثل دور التدقيق الداخلي في الأمور التنفيذية كمستشار ومراقب مستقل.
- **المخاطر والامتثال والقانونية:** تولي مسؤوليات المشاركة في تبني والتأكد من تطبيق مباديء الحوكمة بما يمثل دور تلك الدوائر.
- **حاكمية ورقابة تكنولوجيا المعلومات:**
  - الاشراف على مهام واعمال وواجبات حاكمية عمليات انظمة المعلومات والتكنولوجيا المصاحبة لها بما يضمن توافقها مع افضل الممارسات الدوليه في هذا المجال.
  - تقييم تطبيق وتبني كافة عمليات حاكمية انظمة المعلومات والتكنولوجيا المصاحبة لها والمعتمده ضمن نظام الحاكميه المخصص للبنك والاشراف على وصول وابقاء هذه العمليات ضمن مستويات النضوج

المطلوبه بالاعتماد على اتباع أسلوب تحليل الإنحراف Gap Analysis بين الوضع الحالي ونظام حاكمية وادارة المعلومات والتكنولوجيا المصاحبه لها المعتمد، تحقيقا لاهداف واستراتيجيات البنك.

- توجيه ومراقبة الامتثال لتعليمات البنك المركزي الأردني بهذا الخصوص.
- بناء نظام يضمن متابعة ومراقبة مصفوفة الاهداف المؤسسيه الخاصه بالبنك والية ربطها بمصفوفة اهداف التوافق، واعتمادها ومراجعة هذه الآليه سنوياً وبشكل مستمر مما يضمن تحقيق الأهداف الاستراتيجية للبنك.
- تصميم وبناء نظام حاكمية مخصص لتلبية احتياجات ومتطلبات البنك بناء على دراسة نوعية و/او كمية تعد لهذا الغرض وتراجع بشكل سنوي على الأقل وتأخذ بالاعتبار محددات التصميم (Design Factors) والأهداف ذات الأولوية والاهمية العليا (Focus Area)، وضمان مواءمتها مع اهداف واستراتيجية البنك.
- مراقبة وتحليل أداء عمليات انظمة المعلومات والتكنولوجيا المصاحبة لها عن طريق مؤشرات الاداء.
- رفع المواد والتقارير المناسبه لاجتماعات اللجنة التوجيهيه العليا ولجنة حاكمية تكنولوجيا المعلومات، وضمان شفافية وجودة المعلومات مما يدعم اتخاذ القرارات والتوصيات المناسبه لتحقيق الفائدة، وتعظيم القيمة المضافة لاصحاب المصلحه، ومتابعة إنجاز التكليفات المنبثقة عن هذه اللجان.
- تولي دور المرشد لنشر المعرفة بالمعيار وتسهيل عملية التطبيق والتبني على ان يتم الاستعانه بالمتخصصين وحملة الشهادات الفنيه والمهنيه الخاصه بالمعيار COBIT Foundation, COBIT Assessor, COBIT Implementation, CGEIT من داخل البنك ومن خارجه عند الحاجه.

ثالث عشر: المراجعة والتعديلات:

يتم مراجعة هذا الدليل وتحديثه كلما اقتضت الحاجة وذلك من خلال لجنة حاكمية تكنولوجيا المعلومات المنبثقة عن المجلس.

رابع عشر: مواد ومرفقات التعليمات:

تتلخص المرفقات بمجموعة من المرتكزات والدعامات والأهداف المؤسسيّة وأهداف تكنولوجيا المعلومات والعمليات المرتبطة بها وآليات التدقيق الداخلي والخارجي والنماذج الواجب تطبيقها من خلال البنود الواردة في الدليل اعلاه والمواد (عدد اربعة عشر) والمرفقات التفصيلية (عدد ثمانية) المذكورة والمرفقة في التعليمات وحسب الملخص التالي:

مواد التعليمات:

1.1 تعريف وشروط تطبيق التعليمات (المادة 1)
1.2 التعريفات (المادة 2)
1.3 نطاق التعليمات (المادة 3)
1.4 اعداد دليل حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها (المادة 4)
1.5 نشر دليل حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها (المادة 5)
1.6 اعداد أهداف حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها (المادة 6)
1.7 اللجان المادة (7)
1.8 الأهداف وعمليات حاكمية تكنولوجيا المعلومات (المادة 8)
1.9 التدقيق الداخلي والخارجي (المادة 9)
1.10 المبادئ والسياسات وأطر العمل (المادة 10)
1.11 الهياكل التنظيمية (المادة 11)
1.12 المعلومات والتقارير (المادة 12)
1.13 الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات (المادة 13)
1.14 المعارف والمهارات والخبرات (المادة 14)
1.15 منظومة القيم والأخلاق والسلوكيات (المادة 15)

مرفقات التعليمات:

الملحق 1: تحل الاهداف المؤسسية (Enterprise Goals) (تتكون من 13 هدف) ومؤشرات/معايير قياس مدى تحققها على مستوى كل هدف والمطلوبة من البنوك مكان مصفوفة الاهداف المؤسسية في المرفق (1) من التعليمات

الملحق 2: تحل مصفوفة أهداف التوافق Alignment Goals (تتكون من 13 هدف) ومؤشرات/معايير قياس مدى تحققها والمطلوبة من البنوك مكان مصفوفة الاهداف المؤسسية في المرفق (2) من التعليمات، وتتفق المصفوفة بشكل مباشر او غير مباشر مع الأهداف المؤسسية.

الملحق 3: اهداف حاكمية وإدارة تكنولوجيا المعلومات Governance & Management Objectives، 40 هداف ضمن خمس محاور رئيسية تشكل الاطار العام لحوكمة وادارة عمليات انظمة وتكنولوجيا المعلومات) وحسب الوارد في الصفحة 33-35 من Governance and Management Objectives COBIT 2019

- الحوكمة (مجلس الادارة):

✓ اهداف التقييم والتوجيه والرقابة Evaluate, Direct and Monitor (EDM) وتنقسم الى 5 اهداف

- الادارة التنفيذية (التخطيط، البناء، التشغيل، الرقابة):

✓ اهداف التوافق والتخطيط والتنظيم Align, Plan and Organize (APO) وتنقسم الى 14 اهداف.

✓ اهداف البناء والتطوير والشراء Build, Acquire and Implement (BAI) وتنقسم الى 11 اهداف.

✓ اهداف توصيل الخدمات والدعم Delivery, Service and Support (DSS) وتنقسم الى 6 اهداف.

✓ اهداف الرقابة والتقييم والقياس Monitor, Evaluate and Assess (MEA) وتنقسم الى 4 اهداف.

الملحق 4: نموذج وآليات تقرير تدقيق المعلومات والتكنولوجيا المصاحبة لها وحسب المكونات التالية:

I. نموذج إطلاع وتوصيات المجلس على التقرير
II. الآليات: نتائج التقييم الكلي Composite Risk rating، تقييم (مخاطر ضوابط) المعلومات والتكنولوجيا المصاحبة لها، منهجية الفحص والتقييم، مناقشة التقرير، محددات التدقيق، مؤهلات وخبرات المدقق المسؤول وأعضاء فريق التدقيق
III. متن التقرير
IV. الملاحظات العالقة ولم تعالج من سنوات سابقة

الملحق 5: محاور تدقيق المعلومات والتكنولوجيا المصاحبة لها وبحد أدنى حسب التالي:

حاكمية تكنولوجيا المعلومات IT Governance، البرامج التطبيقية وادارتها، ادارة قواعد البيانات، ادارة اجهزة الكمبيوتر الرئيسية، ادارة الشبكات، ادارة خطط استمرارية الاعمال والامن المادي والبيئي.

الملحق 6: منظومة السياسات المطلوبة وبحد أدنى (26 سياسة رئيسية):

حاكمية تنظيم تكنولوجيا المعلومات، أمن وحماية المعلومات، خطط استمرارية العمل والتعافي من الكوارث، ادارة مخاطر تكنولوجيا المعلومات، الامتثال لسياسات تكنولوجيا المعلومات، خصوصية البيانات Data Privacy، التعهيد Outsourcing، ادارة المشاريع، ادارة الموجودات، الاستخدام والسلوك المقبول لموارد تكنولوجيا المعلومات، ادارة التغيير Change Management، أجهزة الكمبيوتر (المركزية، الطرفية)، الاجهزة المحمولة، ادارة صلاحيات النفاذ User Access Management، سياسة تطوير واقتناء البرمجيات System Development Life Cycle، ادارة مستوى الخدمات Service level management، النسخ الاحتياطية والاسترجاع Back up & Restore، الاحتفاظ بالبيانات Retention، شراء الانظمة والتجهيزات Purchasing، النفاذ عن بعد Remote Access، الشبكات، الشبكات اللاسلكية، فحص الاختراق وتحليل الثغرات Vulnerability Penetration Testing &، اجهزة الحماية Fire walls، مقسم الهاتف.

الملحق 7: المعلومات والتقارير وأسس العمل وبحد أدنى (20 بند):

مصفوفة الصلاحيات والامتيازات Authority Matrix، تحليل عوامل المخاطر IT Risk Factors Analysis، سيناريوهات تحليل مخاطر تكنولوجيا المعلومات IT Risk scenario analysis، سجل مخاطر تكنولوجيا المعلومات IT Risk Register، مصفوفة الادوار والمسؤوليات RACI Chart، ملف المخاطر IT Risk Profile، تقارير المخاطر IT Risk Reports، خريطة المخاطر IT Risk Map، المخاطر المقبولة والكامنة Risk Universe & Appetite & Tolerance، مؤشرات قياس

المخاطر الرئيسية IT Risk Indicators، تعريفات المخاطر Risk Taxonomy، مصفوفة المخاطر المحسوبة Risk and Control Activity Matrix، ميزانيات أمن وحماية المعلومات، تقارير دعم القرار MIS Reports، استراتيجيات تدقيق تكنولوجيا المعلومات، اجراءات تدقيق تكنولوجيا المعلومات، مصفوفة المؤهلات Competencies، أفضل المعايير الدولية لإدارة موارد ومشاريع تكنولوجيا المعلومات، وإدارة مخاطر تكنولوجيا المعلومات، وأمن وحماية والتدقيق على تكنولوجيا المعلومات

الملحق 8: الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات وبحد أدنى (8 بنود):
خدمات ادارة الحوادث Incident Management Services، ادارة موجودات تكنولوجيا المعلومات IT Assets Inventory، التوعية بالممارسات السليمة لأمن المعلومات، ادارة اجراءات النفاذ Access Management، ادارة وحماية المعلومات Information management Systems، مراقبة امن المعلومات، ادارة وضبط البيئات المحيطة بأنظمة وتكنولوجيا المعلومات (غرف الخوادم والاتصالات والكهرباء)، برمجيات تدقيق تكنولوجيا المعلومات

المراجع:

1. تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم 2016/65 بتاريخ 2016/10/25 الصادرة عن البنك المركزي وتعميم البنك المركزي رقم 948/6/10 بتاريخ 2019/1/21 والمستند على الاطار المرجعي COBIT 2019 والمنشور على موقع البنك المركزي http://www.cbj.gov.jo
2. تعليمات COBIT والصادرة من جمعية التدقيق والرقابة على نظم المعلومات في الولايات المتحدة الأمريكية Information Systems Audit and Control Association (ISACA) والمنشور على موقع الجمعية https://www.isaca.org/COBIT/Pages/Product-Family.aspx

- COBIT 5 Framework
- COBIT 5 Implementation
- COBIT 5 Enabling Process
- COBIT 5 Enabling Information
- COBIT 2019 Framework: Introduction and Methodology
- COBIT 2019 Framework: Governance and Management Objectives
- COBIT 2019 Design Guide: Designing and Information and Technology Governance Solution
- COBIT 2019 Implementation Guide: Implementing and Optimizing and Information and Technology Governance Solution