دليل حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها

بنك الإسكان للتجارة والتمويل

الإصدار الرابع

الفهرس

أولاً: المقدّمة

تعتبر موارد تكنولوجيا المعلومات مرتكزاً مهماً من حيث الحجم النسبي ومن حيث التأثير على قدرة المؤسسة في تسيير عملياتها وبالتالي تحقيق أهدافها، كما وتلعب دورا حساساً 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 الإسكان أن يقوم باتباع المرتكزات والمعايير السليمة في إدارة موارد تكنولوجيا المعلومات بحسب الممارسات الدولية المقبولة بهذا الخصوص لتقليل مخاطرها وتجنباً 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 الإسكان 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 الإطار 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) وإطار 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 التزاماً 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. **أهداف حاكمية وإدارة 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** - أهداف 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:** تشمل الرئيس التنفيذي ورؤساء القطاعات ونائب رئيس تنفيذي- مدير إدارة المخاطر ونائب رئيس تنفيذي- المدقق العام ونائب رئيس تنفيذي- مدير إدارة مراقبة الامتثال، ومدراء الإدارات والدوائر أو أي موظف في البنك ممن له سلطة 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 المصاحبة لها رقم 2016/65 والصادرة بتاريخ 2016/10/25 وتعميم البنك المركزي اللاحق رقم 948/6/10 بتاريخ 2019/1/21

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

ل. **المرفقات/الملاحق:** هي المرفقات الواردة في تعليمات البنك المركزي المتعلقة بحاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم 2016/65 والصادرة بتاريخ 2016/10/25 وعددها ثمانية مرفقات على شكل ملاحق مطلوب تطبيقها بالتوافق مع المواد –خمسة عشرة مادة - الواردة في وثيقة التعليمات الرئيسية بالإضافة إلى وثائق إطار العمل المرجعي COBIT 2019 والمعتمد حسب تعميم البنك المركزي رقم 948/6/10 بتاريخ 2019/1/21.

رابعاً: نشر دليل حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها:

يقوم البنك بنشـــر هذا الدليل على موقعه الإلكتروني، وبأي طريقة أخرى مناســـبة لاطلاع الجمهور، كما يتم الإفصـــاح في التقرير السنوي للبنك عن وجود دليل لحاكمية وإدارة المعلومـــات والتكنولوجيـــا المصـــاحبة لها، والإفصاح ايضاً عن المعلومات التي تهم أصحاب المصالح بما فيها الدليل، وعن مدى التزام البنك بتطبيق ما جاء فيه.

خامساً: اللجان:

تم تشـكيل لجنتين أحدهما على مسـتوى مجلس الإدارة وتسـمى "لجنة حاكمية تكنولوجيا المعلومات" والأخرى على مسـتوى الإدارة التنفيذية العليا وتسمى "اللجنة التوجيهية لتكنولوجيا المعلومات":

أ. لجنة حاكمية تكنولوجيا المعلومات:

- تتشكل هذه اللجنة من ثلاثة أعضاء من مجلس الإدارة على الأقل.
- تضم في عضويتها أشخاص من ذوي الخبرة أو المعرفة الاستراتيجية في تكنولوجيا المعلومات.
- تقوم اللجنه بالاســتعانة – عند اللزوم – وعلى نفقة البنك بخبراء خارجيين وذلك بالتنســيق مع رئيس المجلس بفرض تعويض النقص بهذا المجال من جهة ولتعزيز الرأي الموضوعي من جهة أخرى.
- للجنة دعوة أي من إداري البنك لحضـور اجتماعاتها للاسـتعانة برأيهم، بما فيهم المعنيين في التدقيق الداخلي وأعضـاء الإدارة التنفيذية العليا (مثل: نائب رئيس أول- مدير أنظمة المعلومات) أو المعنيين في التدقيق الخارجي.
- يحدد المجلس أهدافهاويفوضها بصلاحيات من قبله، وذلك وفق ميثاق يوضح ذلك.
- تقوم برفع تقارير دورية للمجلس، علماً بأن تفويض المجلس صـلاحيات للجنة لا يعفيه ككل من تحمل مسـؤولياته بهذا الخصوص.
- تجتمع اللجنة بشكل ربع سنوي على الأقل، وتحتفظ بمحاضر اجتماعات موثقة.
- تتولى اللجنة – كحد أدنى - المهام التالية:

1. اعتماد الأهداف الاستراتيجية لتكنولوجيا المعلومات وأهداف 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 الإطار المرجعي COBIT 2019 ويغطي أهداف الحاكمية والإدارة الواردة في الإطار المرجعيCOBIT 2019.

3. اعتماد مصفوفة الأهداف المؤسسية الواردة في الإطار 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 الإطار 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 الأهداف 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 أهداف حاكمية وإدارة تكنولوجيا المعلومات الواردة في الإطار 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 إلى مهامها اعتماد أهمية وترتيب أولوية الأهداف الواردة في الإطار المرجعي COBIT 2019 (Governance & Management Objectives) ومدى ارتباطها مع الأهداف المؤسسية و Alignment Objectives بالإضافة إلى 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 الإدارة التنفيذية العليا ممثلة بـ (رئيس قطاع العمليات، رئيس قطاع الأعمال، رئيس قطاع المالية، نائب رئيس تنفيذي- مدير إدارة المخاطر، نائب رئيس تنفيذي- مدير إدارة الائتمان، نائب رئيس أول- مدير أنظمة المعلومات، مدير أول- مخاطر الأمن السيبراني وأمن المعلومات)، وينتخب المجلس أحد أعضائه ليكون عضواً مراقباً في هذه اللجنة بالإضافة لنائب رئيس تنفيذي- المدقق العام.
- يمكنها دعوة الغير لدى الحاجة لحضور اجتماعاتها.
- توثق اللجنة اجتماعاتها بمحاضر أصولية.
- تكون دورية الاجتماعات مرة كل ثلاثة أشهر على الأقل.
- تتولى اللجنة – كحد أدنى - المهام التالية:

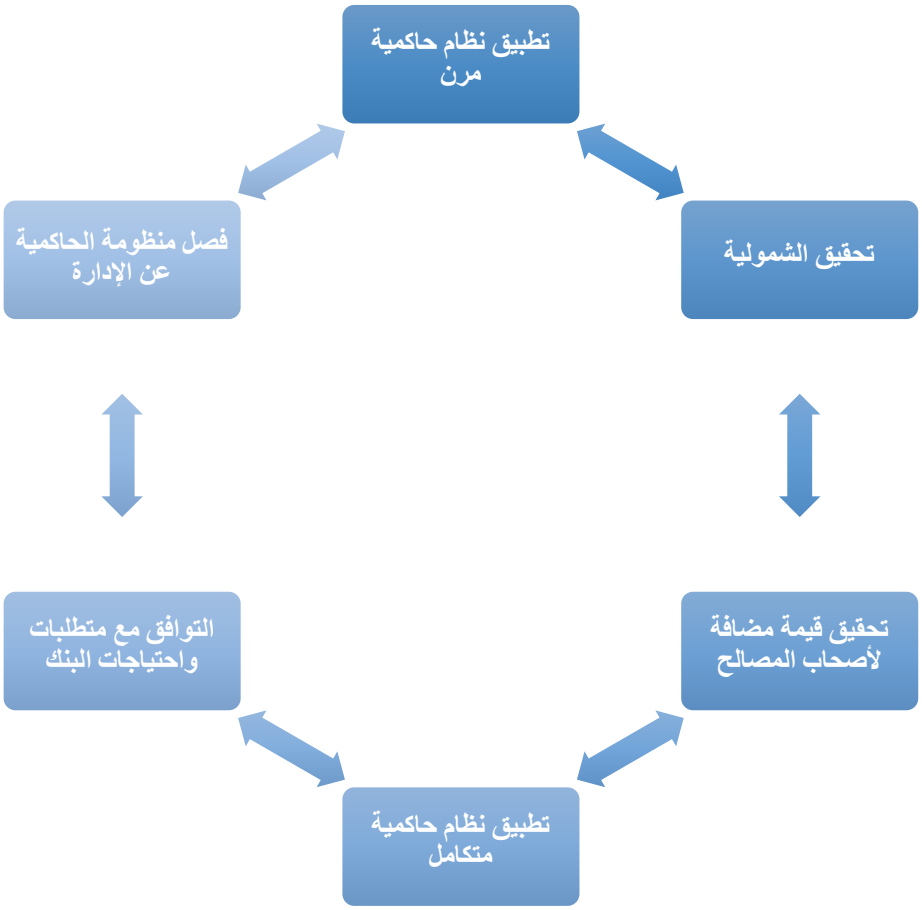
1. وضع الخطط السنوية الكفيلة بالوصول للأهداف الاستراتيجية المقرة من قبل المجلس، والإشراف على تنفيذها لضمان تحقيقها ومراقبة العوامل الداخلية والخارجية المؤثرة عليها بشكل مستمر.

2. ربط مصفوفة الأهداف المؤسسية بمصفوفة Alignment Goals المصاحبة لها 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 (Governance and Management Objectives، Alignment Goals) كحد أدنى من خلال التوصية بتخصيص الموارد المالية وغير المالية اللازمة والاستعانة بالعنصر البشري الكفؤ والمناسب في المكان المناسب من خلال هياكل تنظيمية مقترحة تشمل كافة العمليات والأنشطة اللازمة لدعم الأهداف تراعي فصل المهام وعدم تضارب المصالح، وتطويع البنية التحتيةالتكنولوجية 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 والمخاطرة.
5. الاطلاع على سير عمليات وموارد ومشاريع تكنولوجيا المعلومات وحالة إنجازها للتأكد من كفايتها ومساهمتها الفاعلة في تحقيق متطلبات وأعمال البنك.
6. مراقبة مستوى الخدمات الفنية والتكنولوجية والعمل على رفع كفاءتها وتحسينها بشكل مستمر.
7. تقييم ومراجعة ميزانية الأنظمة السنوية (الرأسمالية والتشغيلية) واستراتيجية الأنظمة لضمان توافقها المستمر مع إستراتيجية الأعمال بشكل نصف سنوي وتقييم المنجزات خلال هذه الفترة، والتوصية بإتخاذ الإجراءات التصحيحية المناسبة.
8. 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 سلباً 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.
    - اعتماد مصفوفة المسؤوليات (RACI Charts) والممارسات تجاه الأهداف/ العمليات الرئيسية لإدارة تكنولوجيا المعلومات والعمليات الفرعية المنبثقة عنها.
9. تزويد لجنة حاكمية تكنولوجيا المعلومات بمحاضر اجتماعاتها أولا بأول والحصول على ما يفيد الاطلاع عليها.
10. اعتماد باقي المكونات الخاصة بوثائق أهداف/ عمليات إدارة تكنولوجيا المعلومات (باستثناء مصفوفات الصلاحيات والممارسات).

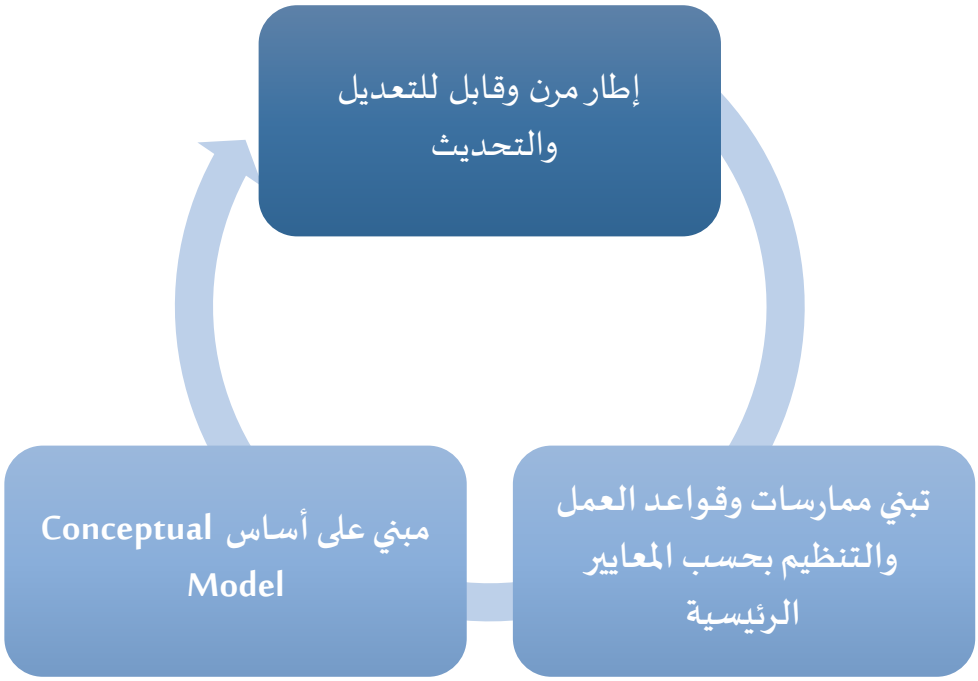
سادساً: مبادئ إطار حاكمية تكنولوجيا المعلومات

تنقسم مبادئ حاكمية تكنولوجيا المعلومات إلى مجموعتين:

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



المجموعة الثانية: المبادئ المرتبطة بإطار 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 وداعمة 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. تحقيق الشمولية في حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها من حيث الأخذ بالاعتبار ليس فقط التكنولوجيا بحد ذاتها وإنما توفير عناصر تمكين (enablers or components) تكون مصاحبة ومكملة لخدمات تكنولوجيا المعلومات تتمثل بـ:

1. المبادئ والسياسات وأطر العمل
2. العمليات/ أهداف حاكمية تكنولوجيا المعلومات.

3. الهياكل التنظيمية.
4. المعلومات و التقارير.
5. الخدمات و البرامج و البنية التحتية لتكنولوجيا المعلومات.
6. المعارف و المهارات و الخبرات.
7. منظومة القيم و الأخلاق و السلوكيات.

و ضرورة توفيرها بمواصفات و أبعاد محددة لتحقيق خدمة متطلبات و أهداف المعلومات و التكنولوجيا المصاحبة لها ليس فقط في عمليات / أهداف تكنولوجيا المعلومات و حسب وإنما في كافة عمليات البنك المرتكزة على المعلومات و التكنولوجيا.

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

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

هـ. 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. المبادئ والسياسات وأطر 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 الإطار 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 وأهداف وعمليات حاكمية تكنولوجيا المعلومات الواردة فيالإطار 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 حداًأدنى 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 إنشاء السياسات مساهمة كافة الشركاء الداخليين والخارجيين واعتماد أفضل الممارساتالدولية 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 الإطار المرجعي COBIT 2019 من حيث: الجهة أو الجهات وتلك المسؤولة بشكل أولي Responsible وتلك المسؤولة بشكل نهائي Accountable وتلك المستشارة Consulted وتلك التي يتم إطلاعها Informed تجاه كافة العمليات في المرفق المذكور مسترشدين بالإطار المرجعي COBIT 2019واعتمادها من قبل اللجان المشار إليها في التعليمات.
- قيام البنك بإعداد اطار عام لإدارة مخاطر تكنولوجيا المعلومات يتوافق ويتكامل مع الإطار العام الكلي لإدارة المخاطر في البنك وبحيث يأخذ بعين الاعتبار ويلبي كافة أهداف حاكمية تكنولوجيا المعلومات الواردة في الإطار المرجعي COBIT 2019.
- قيام البنك بتوفير الوسائل لتحقيق Alignment Goals وأهداف حاكمية تكنولوجيا المعلومات الواردة في الإطار المرجعي COBIT 2019
- تعتبر Alignment Goals وأهداف حاكمية تكنولوجيا المعلومات الواردة في الإطار المرجعي COBIT 2019 ومعطياتها حداً 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 أنظمة لمعلومات المعلومات وإدارة

أمن المعلومات وإدارة المشاريع تحديد عملياتها وإعادة صياغتها بحيث تحاكي وتغطي متطلبات كافة أهداف حاكمية تكنولوجيا المعلومات الواردة في الإطار المرجعي COBIT 2019

- التأكّد من توافق أهداف حاكمية تكنولوجيا المعلومات الواردة الإطار المرجعي COBIT 2019 معAlignment Goals والمساهمة في تحقيقها والتوافق وتحقيق الأهداف المؤسسية الواردة في الإطار المرجعي COBIT
- يتولى المجلس المسؤولية المباشرة لعمليات التقييم والتوجيه والرقابة EDM - Evaluate, Direct & Monitor وحسب الإطار المرجعي COBIT 2019
- يتولى المجلس و إدارة المخاطر المسؤولية المباشرة عن عمليّة ضمان إدارة حصيفة لمخاطر تكنولوجيا المعلومات EDM03 (Ensured Risk optimization) وعملية إدارة 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 أهداف حاكمية تكنولوجيا المعلومات الواردة في الإطار 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 في2019. COBIT
- 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 حداًأدنى، 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 اعتماداً 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 الداخلية والخارجية.
- على الإدارة التنفيذية في البنك الاستمرار برفد موظفيها ببرامج التدريب والتعليم المستمر للحفاظ على مستوى من المعارف والمهارات يلبي ويحقق أهداف حاكمية تكنولوجيا المعلومات الواردة في الإطار 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

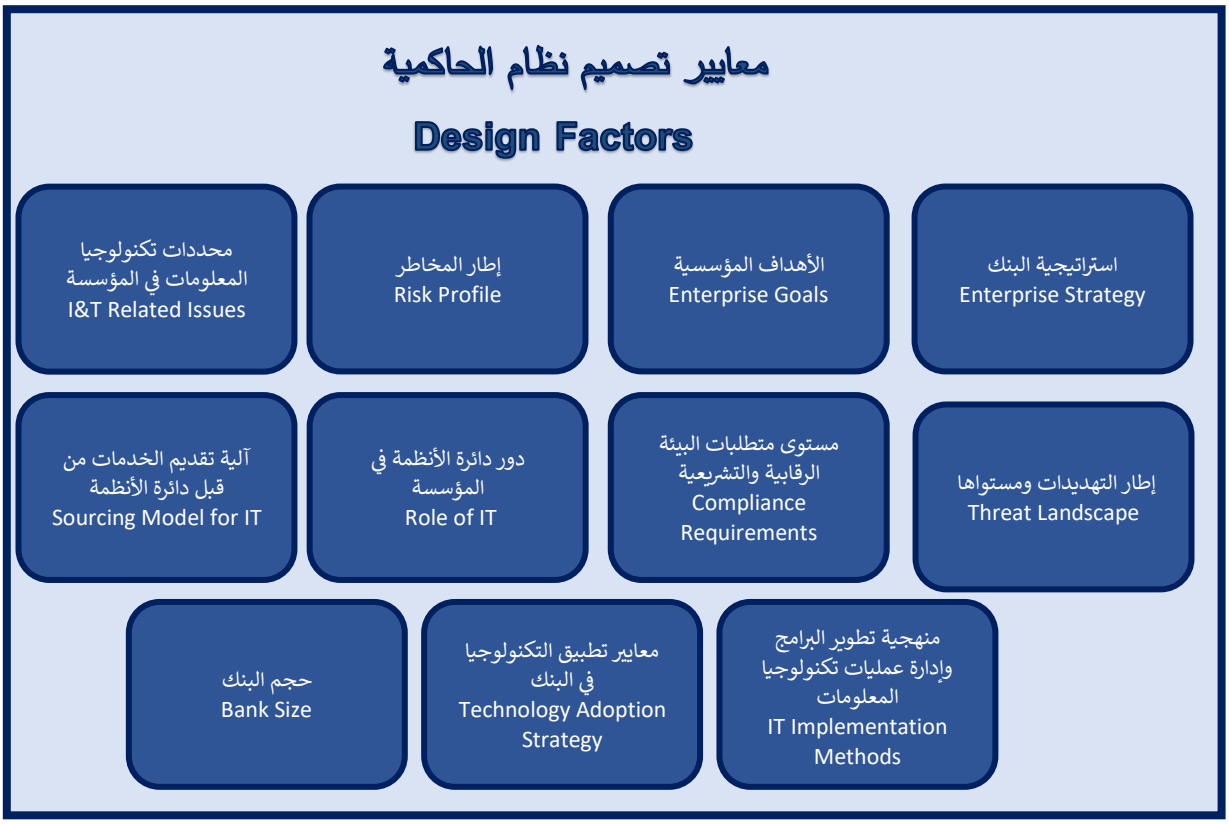
- على المجلس أو من يفُوضّ من لجانه اعتماد منظومة أخلاقية مهنية مؤسسية تعكس القواعد السلوكية المهنية الدولية المقبولة بخصوص التعامل مع المعلومات والتكنولوجيا المصاحبة لها تحدد بوضوح القواعد السلوكية المرغوبة وغير المرغوبة وتبعاتها.
- على المدقق الداخلي والمدقق الخارجي الامتثال لمنظومة الأخلاق والممارسات المهنية المعتمدة من قبل المجلس بحيث تتضمن بالحد الأدنى منظومة الأخلاق المهنية الواردة في المعيار الدولي Information Technology Assurance) (ITAF) (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 أهداف الحاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها بالإضافة إلى مكونات نظام الحاكمية والمرتبطة بنشاطات ومواضيع (الأمن 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 وإدارة المعلومات والتكنولوجيا المصاحبه لها بالاعتماد على منهجيه التصميم الموصى بها في الإطار المرجعي "COBIT 2019 Design Guide"، حيث يتم الأخذ بعين الاعتبار جميع أو بعض من معايير التصميم المذكوره أدناه، من خلال اعطاء وزن لكل خاصيه أو محور كما هو مذكور في الجدول أدناه وبما يتناسب وتقييم وضع البنك واستراتيجيته الحالية:



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 اطارCOBIT2019 وبما يتناسب مع أهداف البنك الاستراتيجية.
.3	إطار 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 أهم الصعوبات التي تواجه دائرة أنظمة المعلومات والتكنولوجيا من خلال قائمة التحديات والصعوبات المذكوره في دليل إطار COBIT2019.
.5	إطار التهديدات ومستواها	– حجم التهديدات التي من الممكن أن يتعرض لها البنك (معتدل) – حجم التهديدات التي من الممكن أن 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 الأعمال – يدعم ويخدم البنك ويؤثر بشكل مباشر على استمرارية الأعمال – دور تطوري وابداعي ولا يؤثر على استمرارية أعمال البنك – دور استراتيجي وداعم لخطط وتطور الأعمال ويؤثر بشكل جوهري على البنك
.8	آلية تقديم الخدمات من قبل دائرة الأنظمة	– 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 أخرى. – 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 إلى إطار حاكمية مؤسسي بالاعتماد على ما يلي:

إحدى 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 دولياً 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 أخرى 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 سنوياً على الأقل في حال تم تقييم المخاطر بدرجة 4 أو 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 اعتمادًعلى 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 تصعيداً تدريجياً 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 ممثلاً بلجنة التدقيق المنبثقة عنه.

5. من الممكن إسناد (Outsource) دور المدقق الداخلي للمعلومات والتكنولوجيا المصاحبة لها (Internal IT Audit) لجهة خارجية متخصصة مستقلة تماماً 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 أو اللجنة القائمة مقامها على أن يتم اطلاع المجلس على تلك التقارير.

اثنى عشر: نطاق وآلية تطبيق وتبني نظام حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها ومهام الأطراف الرئيسية:

أولاً: نطاق وآلية تطبيق وتبني نظام حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة 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 الأهداف الواردة في الإطار المرجعي COBIT 2019 وباقي عناصر التمكين الستة المرتبطة بنشاطات تتعلق بمواضيع الأمن السيبراني وإدارة المخاطر وخصوصية وحماية البيانات والامتثال والمراقبة والتدقيق والتوافق الاستراتيجي عبارة عن Focus Areas ذات أهمية واولوية عليا.
- يجب أن 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 أن لا يقل مستوى النضوج للنشاطات المتعلقة بالأهداف ذات الأهمية والأولوية العليا عن المستوى (3) (Fully Achieved) بحسب سلم النضوج الوارد في الإطار COBIT 2019، ويسمح باعتبار ما لايزيد عن 26% من الأهداف الواردة في الإطار COBIT 2019 ضمن أهداف الإدارة العليا (بما لايزيد عن 9 أهداف بحد أقصى من أصل 35 هدف) على أنها أهداف ذات أهمية واولوية أدنى اعتماد على نتائج دراسة نظام حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها والمعتمدة 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 عناصر التمكين (enablers or components) 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 آخذين 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 لحين الانتهاء من إنجاز كافة بنود التعليمات

ثانياً: الأطراف الرئيسية ومهامها:

- **رئيس وأعضاء المجلس والخبراء الخارجيين المستعان بهم**: تولي مسؤوليات التوجيه العام لتبني والحفاظ على حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها بالمستويات المحددة والموافقة على المهام والمسؤوليات، والدعم وتقديم التمويل اللازم.
- **الرئيس التنفيذي ونوابه ومساعديه ورؤساء القطاعات ومسؤولي العمليات ومدراء الفروع**: تولي مسؤوليات تسمية الأشخاص المناسبين من ذوي الخبرة لتمثيلهم في مشاريع وإدارة عمليات المعلومات والتكنولوجيا المصاحبة لها وتوصيف مهامهم ومسؤولياتهم.
- **لجنة حاكمية تكنولوجيا المعلومات واللجنه التوجيهية لتكنولوجيا المعلومات**: تولي المسؤوليات المنوطة 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.
- **المخاطروالامتثال والقانونية**: تولي مسؤوليات المشاركة في تبني والتأكد من تطبيق مباديء الحوكمة بما يمثل دور تلك الدوائر.
- **وحدة حاكمية تكنولوجيا المعلومات/مركز حاكمية ورقابة تكنولوجيا المعلومات**:
  - إدارة متطلبات االالتزام بمعايير الحاكمية المعتمدة لدى البنك والتحقق من مخرجات إطار الحاكمية لدى البنك وبما يتوافق مع تعليمات حاكمية أنظمة المعلومات والتكنولوجيا المصاحبة لها.
  - تقييم آلية تطبيق وتبني أهداف/ عمليات حاكمية تكنولوجيا المعلومات والمعتمدة ضمن نظام الحاكمية المخصص للبنك والإشراف على وصول العمليات إلى مستويات النضوج المستهدفة لتحقيق أهداف واستراتيجيات البنك وامتثالاً لتعليمات الجهات الرقابية والتأكد من التزام جميع الجهات المعنية بها
  - إعداد دراسة لتصميم نظام الحاكمية (أو مراجعةالدراسةالقائمة) بشكل سنوي لدعم أهداف البنك وبما يتناسب مع الإطار COBIT 2019 وتعليمات البنك المركزي الخاصة بحاكمية تكنولوجيا العلومات ومراجعته واعتماده من لجنة حاكمية تكنولوجيا المعلومات.
  - متابعة ومراقبة تنفيذ عمليات/أهداف تكنولوجيا المعلومات بالتنسيق مع مالكي هذه العمليات والأهداف، جمع ودراسة وتحليل مؤشرات قياس الأداء الخاصة بكل عملية بشكل دوري مع الجهات المعنية وبما يتوافق مع تعليمات حاكمية أنظمة المعلومات والتكنولوجيا المصاحبة لها.
  - الإشراف والمساهمة في إنشاء دليل الخدمات التقنية (IT Service Catalogue) التي تقدمها أنظمة المعلومات إلى الدوائر الأخرى في البنك والإشراف على مراجعته وتعديله بشكل دوري من قبل المعنيين في أنظمة المعلومات والتأكد من توافقه مع متطلبات نظام الحاكمية المرتبطة به بما يتناسب مع الخطة الموضوعة لهذه الغاية.
  - الإشراف والتأكد من تطوير مخرجات عمليات وأهداف نظام حاكمية تكنولوجيا المعلومات المعتمد والتأكد من مراجعتها وصيانتها وفقا لدوريتها.
  - إنشاء وتحديث وثائق تعريف أهداف وعمليات الحاكمية(PDDs - documents definition Process) ومراجعتها بشكل دوري مع المعنيين من مراكز العمل المختلفة.
  - جمع وتحليل البيانات الخاصة بنظام الحاكمية وعمليات الحاكمية وأهدافها من الجهات المعنية داخل البنك وخارجه والتأكد من توافقها مع متطلبات نظام الحاكمية.

- إعداد التقارير والمخرجات والمواد لعرضها على اللجان التوجيهية وحاكمية تكنولوجيا المعلومات وضمان شفافية وجودة المعلومات مما يدعم اتخاذ القرار والتوصيات المناسبة لتحقيق الفائدة وتعظيم القيمة المضافة للبنك وتنسيق اجتماعات اللجنة التوجيهية لتكنولوجيا المعلومات ومتابعة إنجاز التكليفات المنبثقة عن هذه اللجان.
- المشاركة في نشر المعرفة بحاكمية ورقابة تكنولوجيا المعلومات على مستوى البنك وحسب الخطط المعدة لهذه الغاية.
- الاشراف على تطوير ومراجعةالنماذج والمنهجيات وأطر العمل المتعلقة بتكنولوجيا المعلومات والتأكد من كفاية الضوابط الرقابية وبما يوائم أهدافCOBIT والأطر المعتمدة.
- المشاركة في إعداد اتفاقيات مستوى الخدمةالتقنية(OLA,SLA) بين أنظمة المعلومات ومراكز العمل المختلفة في البنك أو بين مراكز العمل داخل أنظمة المعلومات حسب الخطة المعدة سنوياً لهذه الغاية تماشياً مع متطلبات إطار الحاكمية المعتمد بهذا الخصوص.

ثالث عشر: المراجعة والتعديلات:

يتم مراجعة هذا الدليل وتحديثه كلما اقتضت الحاجة وذلك من خلال **وحدة حاكمية تكنولوجيا المعلومات/مركز حاكمية ورقابة تكنولوجيا المعلومات** و اعتماده 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 أعلاه والمواد (عدد خمسة عشر) والمرفقات التفصيلية (عدد ثمانية) المذكورة والمرفقة في التعليمات وحسب الملخص التالي:

مواد التعليمات:

1.1 الإسناد (المادة 1)

1.2 التعريفات (المادة 2)

1.3 نطاق وآلية التطبيق والأطراف المعنية (المادة 3)

1.4 دليل حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها (المادة 4)

1.5 نشر دليل حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها (المادة 5)

1.6 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 الأهداف المؤسسية (Enterprise Goals) (تتكون من 13 هدف) ومؤشرات/معايير قياس مدى تحققها على مستوى كل هدف والمطلوبة من البنوك مكان مصفوفة الأهداف 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 الأهداف المؤسسية في المرفق (2) من التعليمات، وتتفق المصفوفة بشكل مباشر أو غير مباشر مع الأهداف المؤسسية.

الملحق 3: أهداف حاكمية وإدارة تكنولوجيا المعلومات Governance & Management Objectives، 40 هدف ضمن خمس محاور رئيسية تشكل الإطار العام لحوكمة وإدارة عمليات أنظمة وتكنولوجيا المعلومات) وحسب الوارد في الصفحة 33-35 من Governance and Management Objectives COBIT 2019

- <u>الحوكمة (مجلس الإدارة):</u>

✓ أهداف التقييم والتوجيه والرقابة Evaluate, Direct and Monitor (EDM) وتنقسم إلى 5 أهداف

- <u>الإدارة التنفيذية (التخطيط، البناء، التشغيل، الرقابة):</u>

✓ أهداف التوافق والتخطيط والتنظيم Align, Plan and Organize (APO) وتنقسم إلى 14 هدف.

✓ أهداف البناء والتطوير والشراء Build, Acquire and Implement (BAI) وتنقسم إلى 11 هدف.

✓ أهداف توصيل الخدمات والدعم Delivery, Service and Support (DSS) وتنقسم إلى 6 أهداف.

✓ أهداف الرقابة والتقييم والقياس Monitor, Evaluate and Assess (MEA) وتنقسم إلى 4 أهداف.

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

I. نموذج اطلاع 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 وإدارتها، إدارة قواعد البيانات، إدارة أجهزة الكمبيوتر الرئيسية، إدارة الشبكات، إدارة خطط استمرارية الأعمال والأمن 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، إدارة مخاطر تكنولوجيا المعلومات، الامتثال لسياسات تكنولوجيا المعلومات، خصوصية البيانات Data Privacy، التعهيد Outsourcing، إدارة المشاريع، إدارة الموجودات، الاستخدام والسلوك المقبول لموارد تكنولوجيا المعلومات، إدارة التغيير Change Management، أجهزة الكمبيوتر (المركزية، الطرفية)، الأجهزة المحمولة، إدارة صلاحيات النفاذ User Access Management، سياسة تطوير واقتناء البرمجيات System Development Life Cycle، إدارة مستوى الخدمات Service level management، النسخ الاحتياطية والاسترجاع Back up & Restore، الاحتفاظ بالبيانات Retention، شراء الأنظمة والتجهيزات Purchasing، النفاذ عن بعد Remote Access، الشبكات، الشبكات اللاسلكية، فحص الاختراق وتحليل الثغرات Vulnerability & Penetration Testing، أجهزة 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 الأدوار 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، إجراءات 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 إدارة الحوادث Incident Management Services، إدارة موجودات تكنولوجيا المعلومات IT Assets Inventory، التوعية بالممارسات السليمة لأمن المعلومات، إدارة اجراءات النفاذ Access Management، إدارة وحماية المعلومات Information management Systems، مراقبة أمن المعلومات، إدارة 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 الإطار 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 (ISACA) Information Systems Audit and Control Association 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