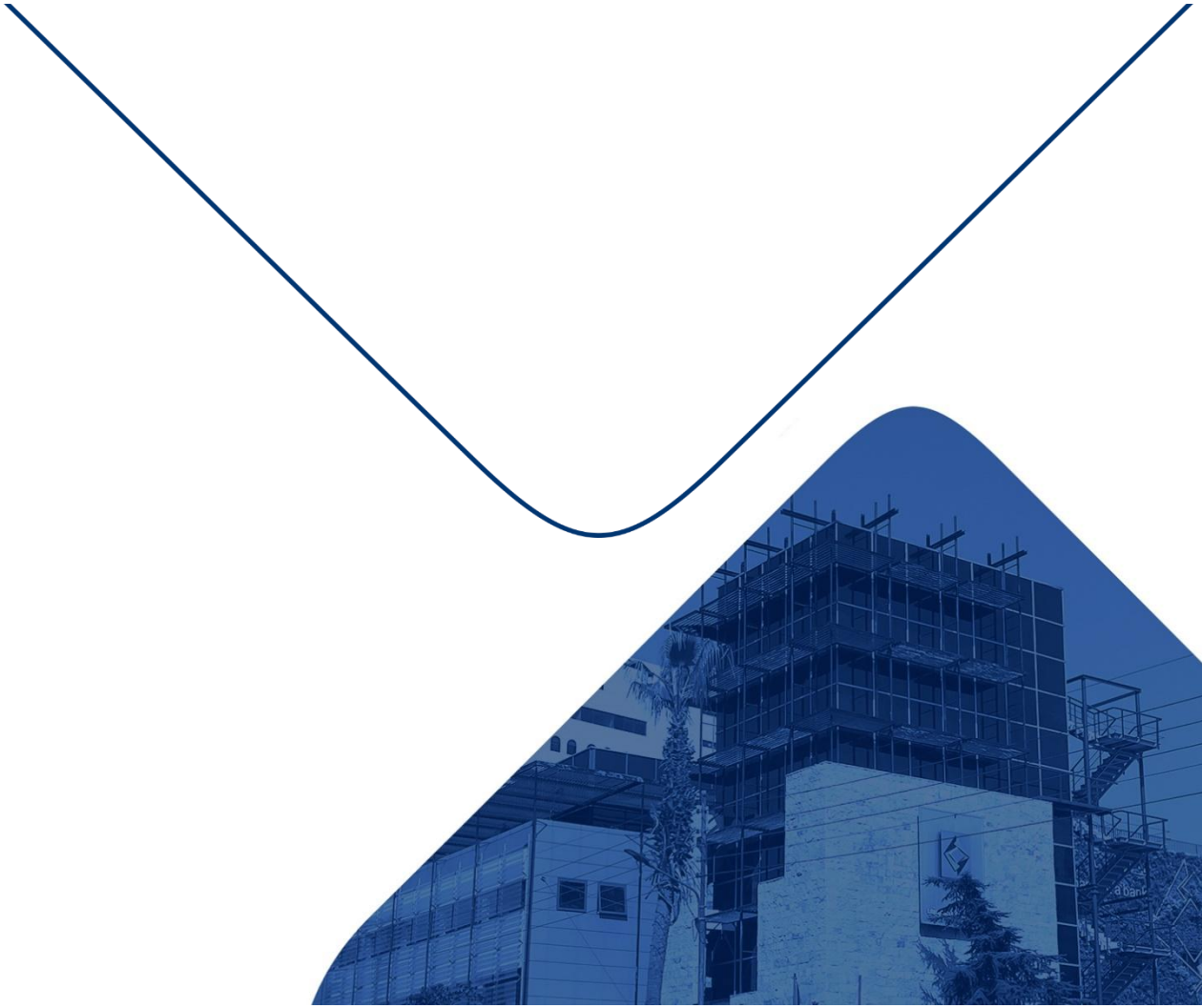
البنك الأردني الكويتي
JORDAN KUWAIT BANK

دليل حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها



جدول المحتويات

مقدمة 3
أولاً: الإسناد 3
ثانياً: التعريفات 4
ثالثاً: نطاق تطبيق الدليل 5
رابعاً: دليل حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها 6
خامساً: نشر دليل حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها: 6
سادساً: أهداف حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها: 6
سابعاً: اللجان 8
ثامناً: الأهداف وعمليات حاكمية تكنولوجيا المعلومات 14
تاسعاً: التدقيق الداخلي والخارجي 15
عاشراً: المبادئ والسياسات وأطر العمل 17
الحادي عشر: الهياكل التنظيمية 17
الثاني عشر: المعلومات والتقارير 17
الثالث عشر: الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات 18
الرابع عشر: المعارف والمهارات والخبرات 18
الخامس عشر: منظومة القيم والأخلاق والسلوكيات 19

مقدمة

لقد تطور مؤخراً دور تكنولوجيا المعلومات من وحدة داعمة الى وحدة أساسية لتحقيق الأهداف الاستراتيجية للمؤسسات، وحيث أن هذه المؤسسات تستند في عملياتها الرئيسية على تكنولوجيا المعلومات كان لا بد من وضع نظام محكم ومتكامل يضمن الاستخدام الفعّال لموارد تكنولوجيا المعلومات من خلال تبني إطار حاكمية وإدارة تكنولوجيا المعلومات.

إن طريقة إدارة موارد تكنولوجيا المعلومات أصبحت عاملا رئيسيا لنجاح المؤسسات بسبب الاعتماد المتزايد على حلول تكنولوجيا المعلومات، وإحدى أبرز هذه الطرق هو تطبيق حاكمية تكنولوجيا المعلومات المؤسسية ممثلا بمعيار **COBIT (Control Objective for Information and related Technology) 2019.**

تعتبر حاكمية تكنولوجيا المعلومات المؤسسية إحدى العمليات التي تسعى إدارة البنك عبرها الى ضبط تنفيذ الاستراتيجيات من خلال السياسات، الأهداف، تفويض الصلاحيات وقياس الأداء. وهي الطريقة المثلى لإدارة عمليات تكنولوجيا المعلومات للاستمرار في تلبية احتياجات الأعمال وأصحاب المصالح من جميع الأطراف على نحو فعال.

تركز حاكمية تكنولوجيا المعلومات في البنك الأردني الكويتي على العديد من العمليات الأساسية مثل إدارة شؤون الموظفين، توفير الموارد، إدارة التغيير، الإدارة المالية، إدارة الجودة، إدارة أمن المعلومات وإنشاء الهياكل التنظيمية الفعالة وفصل الأدوار والمسؤوليات الوظيفية، وإدارة ومراقبة الأداء باستخدام بطاقات الأداء المتوازن لمراقبة هذه العمليات والعمليات الأخرى الرئيسية.

تبدأ حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها من أهداف وسياسات البنك التي يتم ترجمتها الى عمليات وإجراءات وضوابط وأنشطة أخرى تنعكس على جميع مستويات البنك التنظيمية.

أولاً: الإسناد

صدر هذا الدليل سنداً لمتطلبات تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها الصادرة عن البنك المركزي رقم (2016/65) تاريخ 2016/10/25 وتعميم البنك المركزي رقم .984/6/10، وإطار COBIT 2019 الصادر عن جمعية التدقيق والرقابة على نظم المعلومات الامريكية ISACA.

ثانياً: التعريفات

يكون للكلمات والعبارات الواردة في هذا الدليل المعاني المحددة لها فيما بعد ما لم تدل القرينة أو السياق على غير ذلك.

1	البنك	البنك الأردني الكويتي
2	البنك المركزي	البنك المركزي الأردني
3	الدليل	دليل حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها في البنك الأردني الكويتي
4	حاكمية المعلومات والتكنولوجيا المصاحبة لها	توزيع الأدوار والمسؤوليات وتوصيف العلاقات بين الأطراف والجهات المختلفة وأصحاب المصالح (مثل مجلس الإدارة والإدارة التنفيذية) بهدف تعظيم القيمة المضافة للمؤسسة باتباع النهج الأمثل الذي يكفل الموازنة 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.
5	إدارة المعلومات والتكنولوجيا المصاحبة لها	مجموعة النشاطات المستمرة التي تقع ضمن مسؤولية الإدارة التنفيذية وتشمل التخطيط بغرض تحقيق الأهداف الاستراتيجية بما يشمل الموائمة 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.
6	عمليات حاكمية تكنولوجيا المعلومات	مجموعة الممارسات والنشاطات المنبثقة عن سياسات المؤسسة واللازمة لتحقيق أهداف المعلومات والتكنولوجيا المصاحبة لها.
7	أهداف المعلومات والتكنولوجيا المصاحبة لها	مجموعة الأهداف الرئيسية والفرعية المتعلقة بنشاطات الحاكمية والإدارة للمعلومات والتكنولوجيا المصاحبة لها واللازمة لتحقيق الأهداف المؤسسية.
8	الأهداف المؤسسية	مجموعة الأهداف المتعلقة بالحاكمية والإدارة المؤسسية واللازمة لتحقيق احتياجات أصحاب المصالح وأهداف هذه التعليمات.
9	المجلس	مجلس إدارة البنك الأردني الكويتي

10	**الإدارة التنفيذية العليا**	**تشمل المدير العام للبنك ونائب المدير العام ورئيس الخزينة والاستثمار ورئيس الشؤون المالية ورئيس منتجات التجزئة والبنكية الخاصة ورئيس تنمية أعمال الشركات ومستشار دولة الرئيس ورئيس الشؤون القانونية ورئيس الائتمان ورئيس العمليات ورئيس إدارة الموارد البشرية ورئيس إدارة الشؤون الإدارية ورئيس إدارة مراقبة الامتثال ورئيس تكنولوجيا المعلومات ورئيس إدارة المخاطر.**
11	**المدقق**	**الشخص الطبيعي الذي يقوم بإجراءات التدقيق تحت إشراف الشريك المسؤول عن التدقيق ولا يشمل مدقق الخدمات الإضافية خارج نطاق خدمات التدقيق**
12	**أصحاب المصالح**	**أي ذي مصلحة في البنك مثل المساهمين أو الموظفين أو الدائنين أو العملاء أو المزودين الخارجيين أو الجهات الرقابية المعنية**
13	**في الموقع (On-site)**	**مكان العملية في نفس بناية الإدارة العامة للبنك في الأردن**
14	**خارج الموقع (Off-site)**	**مكان العملية في بناية مغايرة لبناية الإدارة العامة للبنك في الأردن لكن بنفس المحافظة.**
15	**قرب الموقع (Near-site)**	**مكان العملية في محافظة مغايرة للمحافظة التي تتواجد فيها الإدارة العامة للبنك في الأردن.**
16	**في الخارج (Off-shore)**	**مكان العملية في بلد مغاير لبلد الإدارة العامة للبنك**

ثالثاً: نطاق تطبيق الدليل

يشمل نطاق تطبيق كافة عمليات البنك المرتكزة على تكنولوجيا المعلومات بمختلف الفروع والإدارات. ويتوجب على كافة أصحاب المصالح مراعاة الامتثال للتعليمات كل بحسب مسماه وموقعه الوظيفي.

الأطراف الرئيسية ومهامها بهذا الخصوص:

رئيس وأعضاء المجلس والخبراء الخارجيين المستعان بهم: تولي مسؤوليات التوجيه العام للمشروع والموافقة على المهام والمسؤوليات ضمن المشروع والدعم وتقديم التمويل اللازم.

المدير العام ونوابه ومساعديه ومدراء العمليات والفروع: تولي مسؤوليات تسمية الأشخاص المناسبين من ذوي الخبرة بعمليات البنك لتمثيلهم بالمشروع وتوصيف مهامهم ومسؤولياتهم.

مدير ولجان تكنولوجيا المعلومات التوجيهية ومدراء المشاريع: تولي مسؤوليات إدارة المشروع وتوجيهه والإشراف عليه بشكل مباشر والتوصية بتوفير الموارد اللازمة لإتمامه والتأكد من الفهم الصحيح من قبل كافة الأطراف للأهداف المؤسسية لحاكمية تكنولوجيا المعلومات.

التدقيق الداخلي: تولي مسؤولياته المنوطة به بموجب التعليمات بشكل مباشر، والمشاركة في المشروع / البرنامج بما يمثل دور التدقيق الداخلي في الأمور التنفيذية كمستشار ومراقب مستقل لتسهيل وإنجاح إتمام المشروع / البرنامج.

إدارات المخاطر وأمن المعلومات والامتثال والقانونية: تولي مسؤوليات المشاركة في المشروع /البرنامج بما يمثل دور تلك الإدارات، والتأكد من تمثيل المشروع / البرنامج من قبل كافة الأطراف المعنية.

المتخصصين وحملة الشهادات الفنية والمهنية الخاصة بالمعيار (COBIT 5 FOUNDATION, COBIT 5 ASSESSOR , COBIT 5 IMPLEMENTATION, CGEIT) المستعان بهم من داخل البنك وخارجه: تولي دور المرشد لنشر المعرفة بالمعيار وتسهيل عملية التطبيق.

كما يلتزم البنك عند توقيع اتفاقيات اسناد مع الغير(OUTSOURCING) لتوفير الموارد البشرية والخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات بهدف تسيير عمليات البنك التأكد من التزام الغير بتطبيق بنود تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها بشكل كلي او جزئي وبالقدر الذي يتناسب مع أهمية وطبيعة عمليات البنك والخدمات والبرامج والبنية التحتية المقدمة قبل واثناء فترة التعاقد ولا يعفى المجلس والإدارة التنفيذية العليا من المسؤولية النهائية لتحقيق متطلبات التعليمات مدار البحث بما في ذلك متطلبات التدقيق المشار اليها في هذا الدليل.

رابعاً: دليل حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها

يعبر هذا دليل عن نظرة البنك الخاصة لحاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها من حيث مفهومها وأهميتها ومبادئها الأساسية وبشكل يراعي التشريعات وأفضل الممارسات الدولية بهذا الشأن ويتم من خلال لجنة حاكمية تكنولوجيا المعلومات والأمن السيبراني المنبثقة عن المجلس مراجعة هذا الدليل وتحديثه كلما اقتضت الحاجة.

خامساً: نشر دليل حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها:

- يقوم البنك بنشر نسخة محدثه من دليل حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها على موقع البنك الإلكتروني أو بأي طريقة أخرى متاحة للجمهور.
- كما يتم الإفصاح في التقرير السنوي للبنك عن وجود دليل خاص لحاكمية وإدارة المعلومات والتكنولوجيا المصاحبة وعن مدى الالتزام بالمعلومات التي تحتويه.

سادساً: أهداف حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها:

يسعى البنك الاردني الكويتي الى تحقيق الأهداف التالية من خلال تبني إطار حاكمية تكنولوجيا المعلومات:

- تلبية احتياجات أصحاب المصالح (Stakeholder's Needs) وتحقيق توجهات وأهداف البنك من خلال تحقيق أهداف المعلومات والتكنولوجيا المصاحبة لها، وبما يضمن:
  - توفير معلومات ذات جودة عالية كمرتكز يدعم آليات صنع القرار في البنك.
  - إدارة حصيفة لموارد ومشاريع تكنولوجيا المعلومات، تعظم الاستفادة من تلك الموارد وتقلل الهدر منها.
  - توفير بنية تحتية تكنولوجية متميزة وداعمه تمكن البنك من تحقيق أهدافه.

- الارتقاء بعمليات البنك المختلفة من خلال توظيف منظومة تكنولوجية كفؤة وذات اعتمادية متميزة.
- إدارة حصيفة لمخاطر تكنولوجيا المعلومات تكفل الحماية اللازمة لموجودات البنك.
- المساعدة في تحقيق الامتثال لمتطلبات القوانين والتشريعات والتعليمات بالإضافة للامتثال لاستراتيجية وسياسات وإجراءات العمل الداخلية.
- تحسين نظام الضبط والرقابة الداخلي.
- تعظيم مستوى الرضا عن تكنولوجيا المعلومات من قبل مستخدميها بتلبية احتياجات العمل بكفاءة وفعالية.
- إدارة خدمات الأطراف الخارجية الموكل إليها تنفيذ عمليات ومهام وخدمات ومنتجات.
- تحقيق الشمولية في حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها من حيث الأخذ بالاعتبار ليس فقط التكنولوجيا بحد ذاتها وإنما توفير المكونات التي تساعد في تحقيق هذه الشمولية والتي تتكامل مع بعضها البعض لتحقيق هذا المفهوم وتتمثل هذه المكونات ب:
  1. العمليات
  2. الهياكل التنظيمية
  3. المبادئ والسياسات وإجراءات العمل
  4. المعلومات
  5. منظومة القيم والأخلاق والسلوكيات
  6. الأشخاص، المهارات والكفاءات
  7. الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات، وضرورة توفيرها بمواصفات وأبعاد محددة لتحقيق وخدمة متطلبات وأهداف المعلومات والتكنولوجيا المصاحبة لها ليس فقط في عمليات تكنولوجيا المعلومات وحسب، وإنما في كافة عمليات البنك المرتكزة على المعلومات والتكنولوجيا

- تبني ممارسات وقواعد العمل والتنظيم بحسب أفضل المعايير الدولية كنقطة انطلاق يتم الارتكاز والبناء عليها في مجالي حاكمية وادارة عمليات ومشاريع تكنولوجيا المعلومات
- تعزيز آليات الرقابة الداخلية والرقابة المستقلة وفحص الامتثال في مجالي حاكمية وادارة المعلومات والتكنولوجيا المصاحبة لها وبما يسهم في تحسين وتطوير الاداء بشكل مستمر.
- فصل عمليات ومهام ومسؤوليات المجلس في مجال الحاكمية عن تلك التي تقع ضمن حدود مسؤولية الإدارة التنفيذية بخصوص المعلومات والتكنولوجيا المصاحبة لها.
- توفير نظام حاكمية مناسب وملائم للبنك من خلال الاعتماد على معايير تصميم محددة يتم من خلالها تحديد مكونات نظام الحاكمية وأولوياتها الواجب اتباعها.

- تغطية كامل العمليات في البنك وعدم التركيز فقط على دور تكنولوجيا المعلومات، بل تغطية كافة العمليات والإجراءات المتعلقة بالمعلومات والتكنولوجيا المصاحبة لها أي كان موقعها في البنك.
- كما وتعتبر أهداف الحاكمية والإدارة وباقي عناصر التمكين الستة المرتبطة بنشاطات تتعلق بمواضيع الامن السيبراني وإدارة المخاطر وخصوصية وحماية البيانات والامتثال والمراقبة والتدقيق والتوافق الاستراتيجي عبارة عن **(FOCUS AREAS)** ذات أهمية وأولوية عليا.

سابعاً: اللجان

أولاً: لجنة مجلس الإدارة لحاكمية تكنولوجيا المعلومات والأمن السيبراني:

لجنة حاكمية تكنولوجيا المعلومات والأمن السيبراني "اللجنة" هي لجنة منبثقة عن مجلس ادارة البنك الأردني الكويتي، تهدف الى مساعدة مجلس الإدارة في وظائفه ودوره الاشرافي لتحقيق أهداف الحاكمية والإدارة في مجال تكنولوجيا المعلومات والأمن السيبراني، بما يضمن توفير معلومات ذات جودة عالية تدعم آليات صنع القرار وإدارة حصيفة لموارد ومشاريع ومخاطر تكنولوجيا المعلومات والمساعدة في تحقيق الامتثال لمتطلبات القوانين والتعليمات والامتثال لاستراتيجية وسياسات واجراءات العمل الداخلية، ووجود اللجنة لا يعفي مجلس الإدارة ككل من تحمل مسؤولياته.

أعضاء اللجنة

- تتألف اللجنة من ثلاثة أعضاء على الأقل ويعين رئيسها بقرار من مجلس الإدارة، ويفضل أن تضم في عضويتها أشخاص من ذوي الخبرة أو المعرفة الاستراتيجية في تكنولوجيا المعلومات، وللجنة الاستعانة عند اللزوم بخبراء خارجيين وذلك بالتنسيق مع رئيس المجلس بغرض تعويض النقص بهذا المجال من جهة ولتعزيز الرأي الموضوعي من جهة أخرى.

- يحظر على رئيس اللجنة تولي رئاسة أكثر من لجنتين من اللجان المنبثقة عن المجلس

صلاحيات اللجنة

- طلب أي بيانات أو معلومات من موظفي البنك الذين يتوجب عليهم التعاون لتوفير هذه المعلومات بشـــكل كامل ودقيق.
- طلب المشورة القانونية، أو المالية، أو الإدارية، أو الفنية من أي مستشار خارجي.
- طلب حضور أي موظف في البنك للحصول على أي إيضاحات ضرورية.

مسؤوليات اللجنة:

- المراجعة الدورية لميثاق عمل اللجنة من أجل تقييم مدى كفايته وبما يمكن اللجنة من القيام بالمهام والمسؤوليات المناطة بها وعرض أية تعديلات لازمة على مجلس الإدارة لإقرارها.
- التوجيه والإشراف على إعداد دليل حاكمية وإدارة تكنولوجيا المعلومات وتحديثه ومراقبة تطبيقه.

- ضمان الامتثال بتحقيق متطلبات أهداف حاكمية وإدارة تكنولوجيا المعلومات.

مهام وواجبات اللجنة

تتولى اللجنة المهام التالية:

❖ **فيما يتعلق بحاكمية تكنولوجيا المعلومات**

- اعتماد الأهداف الاستراتيجية لتكنولوجيا المعلومات والهياكل التنظيمية المناسبة بما في ذلك اللجان التوجيهية على مستوى الإدارة التنفيذية العليا خاصة (اللجنة التوجيهية لتكنولوجيا المعلومات والأمن السيبراني) 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 (ROI) وقياس أثر المساهمة في زيادة الكفاءة المالية والتشغيلية.

- اعتماد الإطار العام لإدارة وضبط ومراقبة موارد ومشاريع تكنولوجيا المعلومات يحاكي أفضل الممارسات الدولية المقبولة بهذا الخصوص وعلى وجه التحديد (COBIT) بحيث يتوافق ويلبي تحقيق أهداف الحاكمية والإدارة(تعديل/ تعميم رقم 984/6/10 تعديل تعليمات حاكمية) من خلال تحقيق الأهداف المؤسسية بشكل مستدام، وتحقيق مصفوفة أهداف المعلومات والتكنولوجيا المصاحبة لها، ويغطي أهداف الحاكمية والإدارة.

- اعتماد مصفوفة الأهداف المؤسسية، وأهداف المعلومات والتكنولوجيا المصاحبة لها وتوصيف الأهداف الفرعية اللازمة لتحقيقها.

- اعتماد مصفوفة المسؤوليات (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 2019) .

- التأكد من وجود إطار عام لإدارة مخاطر تكنولوجيا المعلومات يتوافق ويتكامل مع الإطار العام الكلي لإدارة مخاطر البنك بحيث يأخذ بعين الاعتبار ويلبي كافة أهداف الحاكمية والإدارة.

- اعتماد موازنة موارد ومشاريع تكنولوجيا المعلومات بما يتوافق والأهداف الاستراتيجية للبنك.

- الاشراف العام والاطلاع على سير عمليات وموارد ومشاريع تكنولوجيا المعلومات للتأكد من كفايتها ومساهمتها الفاعلة في تحقيق متطلبات وأعمال البنك.

- الاطلاع على تقارير التدقيق لتكنولوجيا المعلومات واتخاذ ما يلزم من إجراءات لمعالجة الانحرافات.

- التوصية للمجلس باتخاذ الإجراءات اللازمة لتصحيح أية انحرافات.

- اعتماد الخطط لاستراتيجيات تكنولوجيا المعلومات والأهداف المرتبطة بها والتوجيه بخصوص أي انحرافات تؤثر على تحقيق الأهداف الاستراتيجية.
- اعتماد أهمية وترتيب أولوية أهداف الحاكمية والإدارة ومدى ارتباطها بالأهداف المؤسسية وأهداف المعلومات والتكنولوجيا المصاحبة لها بالإضافة لارتباطها بباقي عناصر التمكين (enablers or components) الستة المرتبطة بها بناء على دراسة نوعية أو كمية تعد لهذا الغرض تأخذ بعين الاعتبار (COBIT 2019 – Design Guide).
- التأكد بأن الهياكل التنظيمية الخاصة بإدارة موارد وعمليات ومشاريع ومخاطر تكنولوجيا المعلومات وإدارة أمن المعلومات وإدارة الموارد البشرية تلبي متطلبات حاكمية وإدارة تكنولوجيا المعلومات.
- اعتماد سياسات وعمليات حاكمية وإدارة تكنولوجيا المعلومات ومصفوفة المسؤوليات التابعة لها.
- اعتماد خطة مراقبة وقياس عمليات حاكمية وإدارة تكنولوجيا المعلومات.
- اعتماد مؤشرات الأداء القياسية لعمليات حاكمية وإدارة تكنولوجيا المعلومات (KPIs).
- التوصية باعتماد الموازنة التقديرية لتكنولوجيا المعلومات إلى مجلس الإدارة بعد مراجعتها.
- تقديم التوجيهات بخصوص التقارير المتعلقة بمراقبة وقياس أهداف حاكمية وإدارة تكنولوجيا المعلومات.
- تقديم التوجيهات بخصوص مشاريع تكنولوجيا المعلومات التي تم رفعها من قبل اللجنة التوجيهية لتكنولوجيا المعلومات والأمن السيبراني.
- التوصية والتوجيه بخصوص المخاطر غير المقبولة والمتعلقة بتكنولوجيا المعلومات والتي يتم رفعها من قبل اللجنة التوجيهية لتكنولوجيا المعلومات والأمن السيبراني.
- اعتماد منظومة الخدمات والبرامج والبنية التحتية الداعمة والمساعدة لتحقيق أهداف حاكمية وإدارة تكنولوجيا المعلومات.
- اعتماد منظومة أخلاقية ومهنية ومؤسسية تعكس القواعد السلوكية المهنية الدولية المقبولة بخصوص التعامل مع المعلومات والتكنولوجيا المصاحبة لها.
- اعتماد مصفوفة المؤهلات (HR competencies) اللازمة لتحقيق متطلبات أهداف حاكمية وإدارة تكنولوجيا المعلومات.
- اعتماد منظومة المعلومات والتقارير اللازمة لتحقيق متطلبات أهداف حاكمية وإدارة تكنولوجيا المعلومات.
- الاطلاع على جميع محاضر اجتماعات اللجنة التوجيهية لتكنولوجيا المعلومات والأمن السيبراني.

- اعتماد تقارير المدقق الداخلي والخارجي على حاكمية تكنولوجيا المعلومات أو اللجنة القائمة مقامها على أن يتم اطلاع المجلس على تلك التقارير.

❖ **فيما يتعلق بحاكمية الأمن السيبراني:**

- مراقبة تطبيق برنامج الأمن السيبراني وسياسة واستراتيجية الأمن السيبراني لإدارة المخاطر السيبرانية من خلال فريق حاكمية تكنولوجيا المعلومات.
- التأكد من الالتزام ببرنامج الأمن السيبراني، والالتزام بالسياسات والمعايير والإجراءات الصادرة بالخصوص.
- اعتماد عمليات إدارة المخاطر السيبرانية.
- تحديد الأدوار والمسؤوليات المتعلقة بالأمن السيبراني.
- تقديم الدعم والمشاركة في تقييم مرونة المخاطر السيبرانية، وتقييمات المخاطر، والاتجاهات المتطورة في المخاطر السيبرانية، والتهديدات، وأي مبادرات ذات صلة بالأمن السيبراني.
- الوعي بالتأثيرات القانونية والتشريعيات للمخاطر السيبرانية.
- تقديم الدعم للتوعية بالأمن السيبراني في البنك.
- اعتماد الميزانية والمصادر الكافية لتلبية الالتزام بمتطلبات الأمن السيبراني.
- اعتماد ميثاق عمل اللجنة التوجيهية لتكنولوجيا المعلومات والأمن السيبراني

التوصية لمجلس الإدارة:

- اعتماد الأهداف الاستراتيجية والأهداف المؤسسية المتعلقة بالأمن السيبراني
- اعتماد مستوى مخاطر الأمن السيبراني المقبولة كجزء من المخاطر الكلية المقبولة في البنك لضمان أن تكون المخاطر السيبرانية ضمن الحدود المقبولة للمخاطر الكلية.
- اعتماد برنامج واستراتيجية الأمن السيبراني.
- اعتماد سياسة الأمن السيبراني.

اجتماعات اللجنة

دورية الاجتماعات: تجتمع اللجنة دورياً مرة كل ثلاثة أشهر على الأقل، وتدعى للاجتماع بطلب من مجلس الإدارة أو اثنين من أعضائها، وتدون محاضر اجتماعات اللجنة بشكل أصولي.

النصاب: لا يجوز أن يقل عن (3) أعضاء بما فيهم رئيس اللجنة، ولا يجوز اللجوء لتسمية عضو بديل في حال غياب الأصيل، ويجوز لأعضاء اللجنة حضور اجتماعاتها بواسطة أي من وسائل الاتصال الهاتفي المرئي على أن يصادق رئيس اللجنة وأمين السر على محضر اجتماع اللجنة ونصابه القانوني.

القرارات: تؤخذ القرارات بالأغلبية وفي حال التساوي يرجح الجانب الذي صوت معه رئيس اللجنة.

اعداد التقارير

تقوم اللجنة بعرض محاضر الاجتماعات التي تمت على مجلس إدارة البنك في أقرب اجتماع له بعد انعقاد اجتماع اللجنة لغايات اعتمادها، كما تقوم بتقديم تقرير سنوي حول أعمالها إلى اجتماع الهيئة العامة العادي السنوي.

في حال وجود أي تعارض بين توصيات اللجنة وقرارات مجلس الإدارة يقوم مجلس الإدارة تضمين تقرير الحوكمة بياناً يفصل بوضوح هذه التوصيات وأسباب عدم تقيد مجلس الإدارة بها.

ثانياً: اللجنة التوجيهية لتكنولوجيا المعلومات والأمن السيبراني:

قام البنك بتشكيل اللجنة التوجيهية لتكنولوجيا المعلومات والأمن السيبراني لضمان عملية التوافق الاستراتيجي لتكنولوجيا المعلومات لتحقيق الأهداف الاستراتيجية للبنك وبشكل مستدام.

أعضاء اللجنة

تم تشكيل اللجنة برئاسة الرئيس التنفيذي وعضوية مدراء الإدارة التنفيذية العليا بما في ذلك رئيس العمليات ورئيس تكنولوجيا المعلومات ورئيس إدارة المخاطر ورئيس إدارة الامتثال ورؤساء دوائر الأعمال الهامة ومدير أمن المعلومات ومدير الأمن السيبراني، وينتخب المجلس أحد أعضائه ليكون عضواً مراقباً في هذه اللجنة بالإضافة لرئيس التدقيق الداخلي ويمكن دعوة ذو الاختصاص في مواقع العمل للمشاركة في اجتماعات اللجنة إذا دعت الحاجة لذلك، كما يتم تعيين أمين سر اللجنة من قبل الرئيس التنفيذي.

مسؤوليات ومهام اللجنة

- وضع الخطط السنوية الكفيلة بالوصول للأهداف الاستراتيجية المقرة من قبل مجلس الإدارة، والإشراف على تنفيذها وتخصيص الموارد اللازمة لتحقيقها ومراقبة العوامل الداخلية والخارجية المؤثرة عليها بشكل مستمر.
- ربط مصفوفة الأهداف المؤسسية بمصفوفة أهداف المعلومات والتكنولوجيا المصاحبة لها، واعتمادها ومراجعتها بشكل مستمر وبما يضمن تحقيق الأهداف الاستراتيجية للبنك وأهداف تعليمات حاكمية تكنولوجيا المعلومات، ومراعاة تعريف مجموعة معايير للقياس ومراجعتها وتكليف المعنيين بمراقبتها بشكل مستمر وإطلاع اللجنة على ذلك.
- التوصية بتخصيص الموارد المالية وغير المالية اللازمة لتحقيق الأهداف وعمليات حاكمية تكنولوجيا المعلومات والاستعانة بالعنصر البشري الكفؤ 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.
- ترتيب وتحديد أولويات مشاريع وبرامج تكنولوجيا المعلومات ودعم تنفيذها.

- مراقبة مستوى الخدمات الفنية والتكنولوجية والعمل على رفع كفاءتها وتحسينها بشكل مستمر.
- رفع التوصيات اللازمة للجنة المجلس لحاكمية تكنولوجيا المعلومات بخصوص الأمور التالية:
  - تخصيص الموارد اللازمة والآليات الكفيلة بتحقيق مهام لجنة المجلس لحاكمية تكنولوجيا المعلومات والأمن السيبراني.
  - أية انحرافات قد تؤثر سلباً على تحقيق الأهداف الاستراتيجية.
  - أية مخاطر غير مقبولة أو تزيد عن الحد المسموح متعلقة بتكنولوجيا وأمن وحماية المعلومات، توصي اللجنة بقبولها.
  - تقارير الأداء والامتثال بمتطلبات الإطار العام لإدارة وضبط ومراقبة موارد ومشاريع تكنولوجيا وأمن المعلومات.
- الاطلاع على المشتريات المتعلقة بالمعدات والبرامج الرئيسية لتكنولوجيا المعلومات
- ضمان الامتثال بتحقيق متطلبات وأهداف الحاكمية والادارة.
- التأكد من تحقيق أفضل قيمة مضافة من مشاريع واستثمارات موارد تكنولوجيا المعلومات.
- ضمان الاستخدام الأمثل لموارد تكنولوجيا المعلومات.
- التأكد من التعامل الأمثل مع مخاطر تكنولوجيا المعلومات.
- ضمان وجود سجل شامل خاص بالمخاطر السيبرانية، وضمان تحديثه بشكل مستمر وبحيث يكون متوافق مع ملف مخاطر تكنولوجيا المعلومات.
- اعتماد قوائم الصلاحيات المتعلقة بإدارة الأمن والمخاطر السيبرانية لكافة عمليات إدارة وضبط تلك المخاطر والرقابة والتدقيق عليها.
- الاطلاع على نتائج فحوصات الأمن السيبراني ومتابعة معالجة الثغرات الأمنية المكتشفة.
- مراجعة مستوى مخاطر الأمن السيبراني المقبولة ورفع تقاريرها إلى لجنة مجلس الإدارة لحاكمية تكنولوجيا المعلومات والأمن السيبراني.
- مراجعة برنامج واستراتيجية وسياسات الأمن السيبراني، وضمان دعمهم للأهداف المؤسسية.
- مراجعة عمليات إدارة المخاطر السيبرانية ومؤشرات المخاطر والأداء الرئيسية لبرنامج الأمن السيبراني ورفع تقاريرها إلى لجنة مجلس الإدارة لحاكمية تكنولوجيا المعلومات والأمن السيبراني.
- مراجعة تقارير تقييم مرونة المخاطر السيبرانية ورفع تقاريرها إلى لجنة مجلس الإدارة لحاكمية تكنولوجيا المعلومات والأمن السيبراني.
- ضمان توافر موارد الأمن السيبراني الكافية.
- مراجعة برامج التوعية بالأمن السيبراني ونتائج قياس مدى الفعالية.
- مراجعة التطورات والتهديدات المتعلقة بالمخاطر السيبرانية، ودعم المبادرات المتعلقة بالأمن السيبراني

- المراجعة الدورية لميثاق عمل اللجنة من أجل تقييم مدى كفايته وبما يمكن اللجنة من القيام بالمهام والمسؤوليات المناطة بها وعرض أية تعديلات لازمة على لجنة مجلس الإدارة لحاكمية تكنولوجيا المعلومات لإقرارها.

اجتماعات اللجنة

دورية الاجتماعات: تجتمع اللجنة دورياً بشكل ربع سنوي على الأقل وكلما دعت الحاجة، وتوثق اجتماعاتها بمحاضر أصولية.

النصاب: حضور أغلبية الأعضاء على أن يكون منهم رئيس اللجنة أو من ينوب عنه.

القرارات: تؤخذ القرارات بالأغلبية وفي حال تساوي الأصوات يرجح الجانب الذي صوت معه رئيس اللجنة .

إعداد التقارير

تقوم اللجنة برفع توصياتها ومحاضر اجتماعاتها إلى لجنة حاكمية تكنولوجيا المعلومات والأمن السيبراني المنبثقة عن مجلس الإدارة.

ثامناً: الأهداف وعمليات حاكمية تكنولوجيا المعلومات

- تعتبر أهداف الحاكمية والإدارة ومصفوفة أهداف المعلومات والتكنولوجيا المصاحبة لها بحسب المرفقين (2) و(3) على التوالي من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم(2016/65) ومعطياتها حداً أدنى يتوجب على إدارة البنك العليا الامتثال لها وتحقيقها بشكل مستمر بما يتناسب مع نتائج تصميم نظام الحاكمية اعتمادا على معايير التصميم (Design Factors)، وتعتبر اللجنة التوجيهية لتكنولوجيا المعلومات والأمن السيبراني المسؤول الأول عن ضمان الامتثال بتحقيق متطلباتها، ولجنة حاكمية لتكنولوجيا المعلومات والأمن السيبراني والمجلس ككل المسؤول النهائي بهذا الخصوص، ويتوجب على كافة دوائر البنك وعلى وجه الخصوص تكنولوجيا المعلومات ودائرة أمن المعلومات ودائرة مشاريع تكنولوجيا المعلومات تحديد عملياتها وإعادة صياغتها بحيث تحاكي وتغطي متطلبات كافة أهداف الحاكمية والإدارة الواردة في المرفق رقم (3) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (2016/65).
- يتولى المجلس المسؤولية المباشرة لأهداف الحاكمية والإدارة المتعلقة بالتقييم والتوجيه والرقابة (EDM) الواردة في المرفق رقم (3) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (2016/65).
- يتولى المجلس ودائرة إدارة المخاطر المسؤولية عن هدف "ضمان إدارة حصيفة لمخاطر تكنولوجيا المعلومات " (EDM 03) "، وهدف "إدارة المخاطر" (APO 12) الواردة في المرفق رقم (3) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (2016/65).

تاسعاً: التدقيق الداخلي والخارجي

- على المجلس رصد الموازنات الكافية وتخصيص الأدوات والموارد اللازمة بما في ذلك العنصر البشري المؤهل من خلال أقسام متخصصة 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) ، 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/IEC 17024) و/أو أية معايير أخرى موازية.
- 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 تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (2016/65) الصادرة عن البنك المركزي الأردني، وذلك خلال الربع الأول من كل عام.
- 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 هذه التعليمات.
- 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 الالتزام بما يلي:

1. معايير تدقيق تكنولوجيا المعلومات بحسب أخر تحديث للمعيار الدولي (Information Technology Assurance Framework) (ITAF) 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 والالتزام بخطط التدريب والتعليم المستمر من قبل الكادر المتخصص بهذا الصدد.
- ← الالتزام بمعايير الاستقلالية المهنية والإدارية (Professional and Organizational Independency) وضمان عدم تضارب المصالح الحالية والمستقبلية.
- ← الالتزام 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.

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 خاص يشمل على الأقل المحاور المبينة في المرفق(5) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (2016/65)، على أن يكون تكرار التدقيق لكافة المحاور أو جزء منها كحد أدنى مرة واحدة سنويا على الأقل في حال تم تقييم المخاطر بدرجة (5 أو4) بحسب سلم تقييم المخاطر المعتمد الموضح في المرفق رقم (4) من تعليمات حاكمية وإدارة المعلومات و التكنولوجيا المصاحبة لها رقم (2016/65)،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 (1 أو 2)، 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 تكنولوجيا المعلومات والعنصر البشري ،وآليات وأدوات المراقبة والتحسين والتطوير ،والعمل على توثيق نتائج التدقيق وتقييمها اعتماداً على أهمية الاختلالات و نقاط 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 بتواريخ محددة للتصحيح، مع الاشارة ضمن جدول خاص الى رتبة صاحب المسؤولية في البنك لكل ملاحظة.
3. إجراءات منتظمة لمتابعة نتائج التدقيق للتأكد من معالجة الملاحظات والاختلالات الواردة تقارير المدقق بالمواعيد المحددة، والعمل على رفع مستوى الاهمية والمخاطر تصعيداً تدريجياً في حال عدم الاستجابة ووضع المجلس بصورة ذلك كلما تطلب الامر.
4. تضمين آليات التقييم السنوي (Performance Evaluation) لكوادر تدقيق تكنولوجيا المعلومات بمعايير قياس موضوعية، وعلى أن تتم عمليات التقييم من قبل المجلس ممثلاً بلجنة التدقيق المنبثقة عنه وبحسب التسلسل الإداري التنظيمي لدائرة التدقيق الداخلي.

- من الممكن إسناد دور المدقق الداخلي للمعلومات والتكنولوجيا المصاحبة لها (Internal IT Audit) لجهة خارجية (Outsource) متخصصة مستقلة تماما عن المدقق الخارجي المعتمد بهذا الخصوص واحتفاظ لجنة التدقيق المنبثقة عن المجلس والمجلس نفسه بدورهما فيما يتعلق بفحص الامتثال لهذا الدليل كحد أدنى.

عاشراً: المبادئ والسياسات وأطر العمل

- على المجلس او من يفوض من لجانه اعتماد منظومة المبادئ والسياسات وأطر العمل(Frameworks) اللازمة لتحقيق الإطار العام لإدارة وضبط ومراقبة موارد ومشاريع تكنولوجيا المعلومات وبما يلبي متطلبات مصفوفة أهداف المعلومات والتكنولوجيا المصاحبة لها واهداف الحاكمية والإدارة الواردة في المرفقين أرقام (2) و(3) على التوالي من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (2016/65).
- على المجلس او من يفوض 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 مصفوفة أهداف المعلومات والتكنولوجيا المصاحبة لها أهداف الحاكمية والإدارة الواردة في المرفق رقم (3) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (2016/65).
- على المجلس او من يفوض من لجانه اعتماد منظومة السياسات اللازمة لإدارة موارد وأهداف الحاكمية والإدارة الواردة بالمرفق رقم(6) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (2016/65) ، واعتبار منظومة السياسات هذه حداً أدنى مع إمكانية الجمع والدمج لتلك السياسات ، 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 الممارسات الدولية وتحديثاتها كمراجع لصياغة تلك السياسات مثل(COBIT2019, ISO/IEC 27001/2, ISO 31000, ISO/IEC 38500

ISO/IEC 9126, ISO/IEC 15504, ISO 22301, PCI. DSS, ITIL, Etc.).

الحادي عشر: 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 الحاكمية والإدارة الواردة في المرفق رقم (3) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (2016/65) 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.

الثاني عشر: المعلومات والتقارير

- على المجلس والادارة التنفيذية العليا تطوير البنية التحتية ونظم المعلومات اللازمة لتوفير المعلومات والتقارير لمستخدميها كمرتكز لعمليات اتخاذ القرار في البنك وعليه يجب ان تتوفر متطلبات جودة المعلومات (Information Quality Criteria) والمتمثلة بالمصداقية (Integrity Completeness, Accuracy and Validity or

(Currencyومتطلبات السرية بحسب سياسة تصنيف البيانات ومتطلبات التوافرية والامتثال بتلك المعلومات والتقارير، بالإضافة للمتطلبات الاخرى الواردة في المعيار(COBIT5-Enabling Information) والمتمثلة بال (Objectivity, Believability, Reputation, Relevancy, Appropriate Amount, Concise Representation, Consistent Representation, Interpretability, Understandability, Ease of Manipulation, Restricted Access).

- يقوم المجلس او من يفوض من لجانه باعتماد منظومة من المعلومات والتقارير الواردة في المرفق رقم

(7) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها (2016/65)، 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 ان يتم مراجعتها وتطويرها بشكل مستمر لمواكبة تطور، أهداف وعمليات البنك وبما يتفق وأفضل الممارسات الدولية المقبولة بهذا الخصوص.

الثالث عشر: الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات

- على المجلس او من يفوض 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 او من يفوض من لجانه والادارة التنفيذية العليا اعتماد منظومة الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات الواردة في المرفق رقم (8) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة ل ا رقم (2016/65)، واعتبار تلك المنظومة حداً أدنى، وعلى أن يتم توفيرها وتطويرها بشكل مستمر لمواكبة تطور أهداف وعمليات البنك وبما يتفق وأفضل الممارسات الدولية المقبولة بهذا الخصوص.

الرابع عشر: المعارف والمهارات والخبرات

- على المجلس او من يفوض من لجانه مصفوفة المؤهلات (HR Competencies) وسياسات إدارة الموارد البشرية اللازمة لتحقيق متطلبات أهداف الحاكمية والإدارة الواردة في المرفق رقم (3) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (2016/65) ومتطلبات هذه التعليمات بشكل عام، وضمان وضع الرجل المناسب في المكان المناسب.
- على إدارة البنك توظيف العنصر البشري المؤهل والمدرب من الأشخاص ذوي الخبرة في مجالات إدارة موارد تكنولوجيا المعلومات ودائرة إدارة المخاطر ودائرة 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/أو أية معايير أخرى موازية كل بحسب اختصاصه.

- على الإدارة التنفيذية في البنك الاستمرار برفد موظفيها ببرامج التدريب والتعليم المستمر للحفاظ على مستوى من المعارف والمهارات يلبي ويحقق أهداف الحاكمية والإدارة الواردة في المرفق رقم (3) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (2016/65).
- 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.

الخامس عشر: منظومة القيم والأخلاق والسلوكيات

- يقوم المجلس او من يفوض من لجانه باعتماد منظومة اخلاقية 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 الأخلق المهنية الواردة في المعيار الدولي (Information Technology ITAF) (Assurance Framework الصادر عن جمعية التدقيق والرقابة على نظم المعلومات (ISACA) وتحديثاته.
- على المجلس والإدارة التنفيذية العليا توظيف الاليات المختلفة لتشجيع تطبيق السلوكيات المرغوبة وتجنب السلوكيات غير المرغوبة من خلال اتباع أساليب الحوافز والعقوبات على سبيل المثال لا الحصر.