دليل حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها

قائمة المحتويات

مقدمة

تعتبر موارد تكنولوجيا المعلومات مرتكزاً مهماً من حيث الحجم النسبي والتأثير على قدرة المصرف في تسيير عملياته وبالتالي تحقيق أهدافه، كما وتلعب دوراً حساساً في التأثير على تنافسية منتجات وخدمات البنك من جهة وعلى آليات صنع القرار وإدارة المخاطر من جهة أخرى، الأمر الذي يبرر حجم الاستثمارات الضخمة في قطاع تكنولوجيا المعلومات من قبل المؤسسات المصرفية.

لقد واجهت مؤسسات الأعمال في كافة القطاعات والأنشطة تحديات كبيرة فرضت عليها ضرورة استخدام التقنيات الحديثة والتكنولوجيا المتقدمة، بحيث أصبح ذلك أمراً ومعياراً هاماً في تطور هذه المؤسسات ودافعاً للتعامل معها وللتنافسية في مجالات أعمالها. وقد تطلب ذلك قيام تلك المؤسسات بالاستثمار في تقنيات المعلومات وأنظمتها.

وعلى جانب آخر فلم تسلم تلك الاستثمارات الضخمة والتقنيات المعاصرة من وجود العديد من المخاطر والتهديدات والتحديات التي صاحبتها، حيث افرزت البيئة الجديدة متغيرات لم تكن موجودة من قبل في ظل استخدام الأساليب التقليدية التي تعتمد على النظم اليدوية، حيث برزت اشكال جديدة من المخاطر المصاحبة لاستخدام التكنولوجيا والتقنيات الالكترونية والتي اتسم بها العصر واصبحت المؤسسات تتنافس فيما بينها على السبق في استخدامها، وعليه كان لابد لمصرفنا من اتباع المرتكزات والمعايير السليمة والممارسات الدولية المقبولة في إدارة موارد تكنولوجيا المعلومات لتقليل مخاطرها وتجنباً للدخول في استثمارات غير مجدية أو مصاريف غير مبررة.

يحظى مفهوم حوكمة تقنية المعلومات (IT Governance) باهتمام بالغ على كافة المستويات الحكومية والتشريعية وجهات الإشراف والرقابة ومؤسسات الأعمال على حد سواء ، نظراً لما كشفت عنه الدراسات والبحوث من المنافع والمزايا التي تتحقق على المستوى الاقتصادي الكلي وكذلك على مستوى الوحدات الاقتصادية نتيجة تطبيق قواعد ومعايير ومبادئ الحوكمة الجيدة وقد تمخضت المحاولات المتعمقة لإرساء دعائم حوكمة الشركات ظهور أهمية ملحة لأحد عناصر ومحاور الحوكمة وهو ما أطلق عليه حوكمة تقنية المعلومات والذي يعد التطبيق الجيد لمبادئها وقواعدها ومنهجيتها مدخلاً لحماية أمن المعلومات والخصوصية في المؤسسات الاقتصادية.

أولاً: مرجعية الدليل-الإسناد

صدر هذا الدليل سنداً لمتطلبات تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها الصادرة عن البنك المركزي الاردني رقم (٢٠١٦/٦٥) تاريخ ٢٠١٦/١٠/٢٥ وتعليماته ذات العلاقة النافذة في هذا الخصوص. وتم الاستعانة بمعايير COBIT 2019 و COBIT 5 العالمية في إعداد هذا الدليل.

ثانياً: التعريفات

يكون للكلمات والعبارات الواردة في هذا الدليل المعاني المحددة لها فيما بعد ما لم تدل القرينة أو السياق على غير ذلك.		
١.	**البنك**	البنك الإسلامي الأردني.
٢.	**البنك المركزي**	البنك المركزي الأردني.
٣.	**الدليل**	دليل حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها في البنك الإسلامي الأردني.
٤.	**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.
٥.	**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.
٦.	**عمليات حاكمية تكنولوجيا المعلومات**	مجموعة الممارسات والنشاطات المنبثقة عن سياسات المؤسسة واللازمة لتحقيق أهداف المعلومات والتكنولوجيا المصاحبة لها.
٧.	**أهداف المعلومات والتكنولوجيا المصاحبة لها**	مجموعة الأهداف الرئيسية والفرعية المتعلقة بنشاطات الحاكمية والإدارة للمعلومات والتكنولوجيا المصاحبة لها واللازمة لتحقيق الأهداف المؤسسية.
٨.	**الأهداف المؤسسية**	مجموعة الأهداف المتعلقة بالحاكمية والإدارة المؤسسية واللازمة لتحقيق احتياجات أصحاب المصالح وأهداف هذه التعليمات.
٩.	**المجلس**	مجلس إدارة البنك الإسلامي الأردني.
١٠.	**الإدارة التنفيذية العليا**	تشمل الرئيس التنفيذي /المدير العام للبنك ونائب المدير العام ومساعد المدير العام ومدير الدائرة المالية ومدير دائرة العمليات الخارجية ومدير دائرة العمليات المركزية (المحلية) ومدير دائرة إدارة المخاطر ومدير دائرة الخزينة ومدير دائرة مراقبة الامتثال، بالإضافة الى أي موظف في البنك له سلطة تنفيذية موازية لأي من سلطات أي من المذكورين ويرتبط وظيفيا مباشرة بالرئيس التنفيذي /المدير العام.
١١.	**المدقق**	الشخص الطبيعي الذي يقوم بإجراءات التدقيق تحت إشراف الشريك

		المسؤول عن التدقيق ولا يشمل مدقق الخدمات الإضافية خارج نطاق خدمات التدقيق.
١٢.	أصحاب المصالح	أي ذي مصلحة في البنك مثل المساهمين أو الموظفين أو الدائنين أو العملاء أو المزودين الخارجيين أو الجهات الرقابية المعنية.
١٣.	في الموقع (On-site)	مكان العملية في نفس بناية الإدارة العامة للبنك في الأردن.
١٤.	خارج الموقع (Off-site)	مكان العملية في بناية مغايرة لبناية الإدارة العامة للبنك في الأردن لكن بنفس المحافظة.
١٥.	قرب الموقع (Near-site)	مكان العملية في محافظة مغايرة للمحافظة التي تتواجد فيها الإدارة العامة للبنك في الأردن.
١٦.	في الخارج (Off-shore)	مكان العملية في بلد مغاير لبلد الإدارة العامة للبنك.

ثالثاً: نطاق تطبيق الدليل

يشمل نطاق التطبيق كافة عمليات البنك المرتكزة على تكنولوجيا المعلومات بمختلف الفروع والإدارات.

ثالثاً: الالتزام بحاكمية ادارة المعلومات والتكنولوجيا المصاحبة لها

١. تتشكل لجنة منبثقة عن المجلس تسمى "لجنة حاكمية تكنولوجيا المعلومات"، تتألف من ثلاثة اعضاء على الاقل من المجلس والاستعانة عند اللزوم بخبراء خارجيين، وتتولى اللجنة اعتماد الاهداف الاستراتيجية لتكنولوجيا المعلومات والهياكل التنظيمية المناسبة وكذلك وضع الإطار العام لإدارة وضبط ومراقبة موارد ومشاريع تكنولوجيا المعلومات واعتماد مصفوفة الاهداف والمسؤوليات واعتماد الميزانيات للمشاريع والاشراف العام على سير عمليات وموارد ومشاريع تكنولوجيا المعلومات وتحقيقها لمتطلبات واعمال البنك.

٢. تشكيل لجنة من الادارة العليا التنفيذية تسمى "اللجنة التوجيهية لتكنولوجيا المعلومات" برئاسة المدير العام وعضوية مدراء الادارة التنفيذية العليا وتتولى اللجنة وضع الخطط السنوية والتوصية بتخصيص الموارد المالية وغير المالية اللازمة لتحقيق الاهداف والعمل على ترتيب مشاريع وبرامج تكنولوجيا المعلومات بحسب الاولوية وكذلك مراقبة مستوى الخدمات الفنية والتكنولوجية والعمل على رفع كفاءتها وتحسينها.

٣. تضمين تقرير مجلس الادارة السنوي بتقرير للجمهور يبين وجود الدليل ويوضح مدى الالتزام ببنوده، مع ذكر أسباب عدم الالتزام بأي بند لم يتم تطبيقه.

٤. يوفر البنك النسخة المعتمدة من الدليل على الموقع الإلكتروني للبنك www.jordanislamicbank.com

٥. يخضع هذا الدليل للمراجعة كلما دعت الحاجة لذلك.

رابعاً: أهداف حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها

يهدف هذا الدليل إلى تحقيق ما يلي:

١. تلبية احتياجات أصحاب المصالح (Stakeholder's Needs) وتحقيق توجهات وأهداف البنك من خلال تحقيق أهداف المعلومات والتكنولوجيا المصاحبة لها، وبما يضمن:
   أ. توفير معلومات ذات جودة عالية كمرتكز يدعم آليات صنع القرار في البنك.
   ب. إدارة حصيفة لموارد ومشاريع تكنولوجيا المعلومات، تعظم الاستفادة من تلك الموارد وتقلل الهدر منها.
   ج. توفير بنية تحتية تكنولوجية متميزة وداعمه تمكن البنك من تحقيق أهدافه.
   د. الارتقاء بعمليات البنك المختلفة من خلال توظيف منظومة تكنولوجية كفؤة وذات اعتمادية متميزة.
   هـ. إدارة حصيفة لمخاطر تكنولوجيا المعلومات تكفل الحماية اللازمة لموجودات البنك.
   و. المساعدة في تحقيق الامتثال لمتطلبات القوانين والتشريعات والتعليمات بالإضافة للامتثال لاستراتيجية وسياسات وإجراءات العمل الداخلية.
   ز. تحسين نظام الضبط والرقابة الداخلي.
   ح. تعظيم مستوى الرضا عن تكنولوجيا المعلومات من قبل مستخدميها بتلبية احتياجات العمل بكفاءة وفعالية.
   ط. إدارة خدمات الأطراف الخارجية الموكل إليها تنفيذ عمليات ومهام وخدمات ومنتجات.
   ي. 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:
      ١. العمليات.
      ٢. الهياكل التنظيمية.
      ٣. المبادئ والسياسات وإجراءات العمل.
      ٤. المعلومات.
      ٥. منظومة القيم والأخلاق والسلوكيات.
      ٦. الأشخاص، المهارات والكفاءات.
      ٧. 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.
٢. توفير نظام حاكمية ملائم وديناميكي يتم تحديثه باستمرار حسب المتغيرات مثل تعديل توجهات استراتيجية او تكنولوجية.
٣. فصل عمليات ومهام ومسؤوليات المجلس في مجال الحاكمية عن تلك التي تقع ضمن حدود مسؤولية الإدارة التنفيذية بخصوص المعلومات والتكنولوجيا المصاحبة لها.
٤. توفير نظام حاكمية مناسب وملائم لمصرفنا من خلال الاعتماد على معايير تصميم محددة يتم من خلالها تحديد مكونات نظام الحاكمية وأولوياتها الواجب اتباعها.

٥. تغطية كامل العمليات في مصرفنا وعدم التركيز فقط على دور تكنولوجيا المعلومات أنما يتطرق الى كافة العمليات والإجراءات المتعلقة بالمعلومات والتكنولوجيا المصاحبة لها أي كان موقعها في مصرفنا.

خامساً : اللجان

١. لجنة حاكمية تكنولوجيا المعلومات

على المجلس تشكيل لجنة حاكمية تكنولوجيا المعلومات من بين أعضائه، وتتشكل هذه اللجنة من ثلاثة أعضاء على الأقل ويفضل أن يكون في عضويتها أشخاص من ذوي الخبرة والمعرفة الإستراتيجية بتكنولوجيا المعلومات وعلى اللجنة الاجتماع بشكل ربع سنوي على الأقل وتحتفظ بمحاضر اجتماعات موثقة وتتولى المهام التالية كحد أدنى:

أ. اعتماد الأهداف الاستراتيجية لتكنولوجيا المعلومات 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 (ROI) (Return On Investment) ، وقياس أثر المساهمة في زيادة الكفاءة المالية والتشغيلية.

ب. أعتماد أولوية وترتيب أهداف الحاكمية والإدارة ومدى ارتباطها بمصفوفة الأهداف المؤسسية الواردة في المرفق رقم (١) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (٢٠١٦/٦٥) واهداف المعلومات والتكنولوجيا المصاحبة لها الواردة في المرفق رقم (٢) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (٢٠١٦/٦٥) بالإضافة الى مدى ارتباطها بباقي عناصر التمكين / مكونات نظام الحاكمية بناء على دراسة نوعية / كمية تعد لهذا الغرض بشكل سنوي على الأقل تأخذ بعين الإعتبار معايير التصميم (Design Factors) الواردة في (COBIT 2019 – Design Guide) .

ج. اعتماد الإطار العام لإدارة وضبط ومراقبة موارد ومشاريع تكنولوجيا المعلومات يحاكي أفضل الممارسات الدولية المقبولة بهذا الخصوص وعلى وجه التحديد (COBIT) (Control Objectives for Information and related Technology)، يتوافق ويلبي تحقيق أهداف ومتطلبات التعليمات من خلال تحقيق مصفوفة الأهداف المؤسسية الواردة في المرفق رقم (١) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (٢٠١٦/٦٥) بشكل مستدام، وتحقيق مصفوفة أهداف المعلومات والتكنولوجيا المصاحبة لها والواردة في المرفق رقم (٢) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (٢٠١٦/٦٥)، ويغطي أهداف الحاكمية والإدارة الواردة في المرفق رقم (٣) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (٢٠١٦/٦٥).

د. اعتماد مصفوفة الأهداف المؤسسية الواردة في المرفق رقم (١) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (٢٠١٦/٦٥)، ومصفوفة أهداف المعلومات والتكنولوجيا المصاحبة لها الواردة في المرفق رقم (٢) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا

المصاحبة لها رقم (٢٠١٦/٦٥) واعتبار معطياتها حداً أدنى، وتوصيف الأهداف الفرعية اللازمة لتحقيقها.

هـ. اعتماد مصفوفة للمسؤوليات (RACI Chart) تجاه العمليات الرئيسية لحاكمية تكنولوجيا المعلومات في المرفق رقم (٣) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (٢٠١٦/٦٥) 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 إطلاعها (Informed) تجاه كافة العمليات في المرفق المذكور مسترشدين بمعيار (COBIT 5 Enabling Processes) بهذا الخصوص.

و. 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 الحاكمية والإدارة تلك الواردة في المرفق رقم (٣) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (٢٠١٦/٦٥).

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

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

ط. الإطلاع على تقارير التدقيق لتكنولوجيا المعلومات واتخاذ ما يلزم من إجراءات لمعالجة الإنحرافات.

ي. التوصية للمجلس باتخاذ الإجراءات اللازمة لتصحيح أية إنحرافات.

٢. **اللجنة التوجيهية لتكنولوجيا المعلومات:**

على الإدارة التنفيذية العليا تشكيل اللجان التوجيهية اللازمة لضمان عملية التوافق الاستراتيجي لتكنولوجيا المعلومات لتحقيق الأهداف الاستراتيجية للبنك وبشكل مستدام، وعليه تمَّ تشكيل لجنة سميت باللجنة التوجيهية لتكنولوجيا المعلومات ويرأسها المدير العام وعضوية مدراء الإدارة التنفيذية العليا بما في ذلك مدير تكنولوجيا المعلومات ومدير دائرة إدارة المخاطر ومدير دائرة أمن المعلومات، وينتخب المجلس أحد أعضائه ليكون عضواً مراقباً في هذه اللجنة بالإضافة لمدير التدقيق الداخلي، ويمكنها دعوة الغير لدى الحاجة لحضور اجتماعاتها، وتوثق اللجنة اجتماعاتها بمحاضر أصولية، على أن تكون دورية الاجتماعات مرة كل ثلاثة أشهر على الأقل، وتتولى على وجه الخصوص القيام بالمهام التالية:

١. وضع الخطط السنوية الكفيلة بالوصول للأهداف الاستراتيجية المقرة من قبل المجلس، والإشراف على تنفيذها لضمان تحقيقها ومراقبة العوامل الداخلية والخارجية المؤثرة عليها بشكل مستمر.
٢. ربط مصفوفة الأهداف المؤسسية بمصفوفة أهداف المعلومات والتكنولوجيا المصاحبة لها وكما وردت في المرفق رقم (1) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (٢٠١٦/٦٥) 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.
٣. التوصية بتخصيص الموارد المالية وغير المالية اللازمة لتحقيق مصفوفة أهداف المعلومات والتكنولوجيا المصاحبة له وأهداف الحاكمية والإدارة الواردة في المرفقين (٢) و (٣) على التوالي من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (٢٠١٦/٦٥) وكحد أدنى، 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، وتولّي عمليات الإشراف على سير تنفيذ مشاريع وعمليات حاكمية تكنولوجيا المعلومات.
٤. ترتيب مشاريع وبرامج تكنولوجيا المعلومات بحسب الأولوية.
٥. مراقبة مستوى الخدمات الفنية والتكنولوجية والعمل على رفع كفاءتها وتحسينها بشكل مستمر.
٦. رفع التوصيات اللازمة للجنة حاكمية تكنولوجيا المعلومات المنبثقة عن المجلس بخصوص الأمور التالية:
   أ- تخصيص الموارد اللازمة والآليات الكفيلة بتحقيق مهام لجنة حاكمية تكنولوجيا المعلومات.
   ب- أية انحرافات قد تؤثر سلبا على تحقيق الأهداف الاستراتيجية.
   ج- أية مخاطر غير مقبولة متعلقة بتكنولوجيا وأمن وحماية المعلومات.
   د- تقارير الأداء والامتثال بمتطلبات الإطار العام لإدارة وضبط ومراقبة موارد ومشاريع تكنولوجيا المعلومات.

٧. تزويد لجنة حاكمية تكنولوجيا المعلومات بمحاضر اجتماعاتها أولا بأول والحصول على ما يفيد الاطلاع عليها.

سادساً: مصفوفة أهداف المعلومات والتكنولوجيا المصاحبة لها وأهداف الحاكمية والإدارة

١. تعتبر أهداف الحاكمية والإدارة ومصفوفة اهداف المعلومات والتكنولوجيا المصاحبة لها بحسب المرفقين (٢) و(٣) على التوالي من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (٢٠١٦/٦٥) 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 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 تكنولوجيا المعلومات و دائرة أمن المعلومات ودائرة مشاريع تكنولوجيا المعلومات تحديد عملياتها وإعادة صياغتها بحيث تحاكي وتغطي متطلبات كافة أهداف الحاكمية والإدارة الواردة في المرفق رقم (٣) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (٢٠١٦/٦٥).

٢. يتولى المجلس المسؤولية المباشرة لأهداف الحاكمية والإدارة المتعلقة بالتقييم والتوجية والرقابة (EDM) (Evaluate, Direct and Monitor) الواردة في المرفق رقم (٣) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (٢٠١٦/٦٥).

٣. يتولى المجلس ودائرة إدارة المخاطر المسؤولية المباشرة عن هدف "ضمان إدارة حصيفة لمخاطر تكنولوجيا المعلومات" (EDM 03)، وهدف "إدارة المخاطر" (APO 12) الواردة في المرفق رقم (٣) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (٢٠١٦/٦٥).

سابعاً : التدقيق الداخلي والخارجي

١. 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.

٢. 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 (٢٠١٦/٦٥) الصادرة عن البنك المركزي الأردني، وذلك خلال الربع الأول من كل عام.

٣. 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.

٤. 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:

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

١) تنفيذ مهمات التدقيق ضمن خطة معتمدة بهذا الخصوص تأخذ بعين الاعتبار الأهمية النسبية للعمليات ومستوى المخاطر ودرجة التأثير على أهداف ومصالح البنك.

٢) توفير والالتزام بخطط التدريب والتعليم المستمر من قبل الكادر المتخصص بهذا الصدد.

٣) الالتزام بمعايير الاستقلالية المهنية والإدارية (Professional and Organizational Independency) وضمان عدم تضارب المصالح الحالية والمستقبلية.

٤) 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.

ب. 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 رقم (٥) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (٢٠١٦/٦٥)، على أن يكون تكرار التدقيق لكافة المحاور أو جزء منها كحد أدنى مرة واحدة سنويا على الأقل في حال تم تقييم المخاطر بدرجة (٥ أو٤) بحسب سلم تقييم المخاطر المعتمد الموضح في المرفق رقم (٤) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (٢٠١٦/٦٥)، ومرة واحدة كل سنتين على الأقل في حال تم تقييم المخاطر بدرجة (٣)، ومرة واحدة كل ثلاث سنوات على الأقل في حال تم تقييم المخاطر بدرجة (٢ أو١)، 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 بتواريخ محددة للتصحيح، مع الإشارة ضمن جدول خاص إلى رتبة صاحب المسؤولية في البنك مالك كل ملاحظة.

ج. 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.

د. 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.

٥. 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.

ثامناً : المبادئ والسياسات وأطر العمل

١. على المجلس أن يقوم بتفويض لجنة حاكمية تكنولوجيا المعلومات باعتماد 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 (٢) و(٣) على التوالي من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (٢٠١٦/٦٥).

٢. على المجلس أن يقوم بتفويض لجنة حاكمية تكنولوجيا المعلومات باعتماد 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 له أهداف الحاكمية والإدارة الواردة في المرفق رقم (٣) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (٢٠١٦/٦٥).

٣. على المجلس أن يقوم بتفويض لجنة حاكمية تكنولوجيا المعلومات باعتماد منظومة السياسات اللازمة لإدارة موارد وأهداف الحاكمية والإدارة الواردة بالمرفق رقم (٦) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (٢٠١٦/٦٥) ، 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.

٤. يراعى لدى إنشاء السياسات مساهمة كافة الشركاء الداخليين والخارجيين واعتماد أفضل الممارسات الدولية وتحديثاتها كمراجع لصياغة تلك السياسات مثل (COBIT5, ISO/IEC 27001/2, ISO 31000, ISO/IEC 38500, ISO/IEC 9126, ISO/IEC 15504, ISO 22301, PCI DSS, ITIL, ...etc).

تاسعاً : الهياكل التنظيمية

١. 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 (٣) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (٢٠١٦/٦٥) وتحقيق أهداف البنك بكفاءة وفعالية.

٢. يراعى ضمان فصل المهام المتعارضة بطبيعتها ومتطلبات الحماية التنظيمية المتعلقة بالرقابة الثنائية كحد أدنى وكفاية وتحديث الوصف الوظيفي لدى اعتماد وتعديل الهياكل التنظيمية للبنك.

عاشراً: المعلومات

١. 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 المعيار (COBIT 5 – Enabling Information) والمتمثلة بال (Objectivity, Believability, Reputation, Relevancy, Appropriate Amount, Concise Representation, Consistent Representation, Interpretability, Understandability, Ease of Manipulation, Restricted Access).

٢. يقوم المجلس بتفويض لجنة حاكمية تكنولوجيا المعلومات باعتماد منظومة من المعلومات والتقارير الواردة في المرفق رقم (٧) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (٢٠١٦/٦٥)، 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.

حادي عشر: الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات

١. على المجلس أن يقوم ب:

a. تفويض لجنة حاكمية تكنولوجيا المعلومات والإدارة التنفيذية العليا باعتماد منظومة الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات الداعمة والمساعدة لتحقيق عمليات حاكمية تكنولوجيا المعلومات وبالتالي أهداف المعلومات والتكنولوجيا المصاحبة لها، وبالتالي الأهداف المؤسسية.

b. تفويض لجنة حاكمية تكنولوجيا المعلومات والإدارة التنفيذية العليا باعتماد منظومة الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات الواردة في المرفق رقم (٨) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (٢٠١٦/٦٥) ، 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.

ثاني عشر: الاشخاص، المهارات والكفاءات

١. على المجلس أن يقوم بتفويض لجنة حاكمية تكنولوجيا المعلومات باعتماد مصفوفة المؤهلات (HR Competencies) وسياسات إدارة الموارد البشرية اللازمة لتحقيق متطلبات أهداف الحاكمية والإدارة الواردة في المرفق رقم (٣) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (٢٠١٦/٦٥) ومتطلبات هذه التعليمات بشكل عام، وضمان وضع الرجل المناسب في المكان المناسب.

٢. 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 اعتمادا 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.

٣. 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 (٣) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (٢٠١٦/٦٥).

٤. 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.

ثالث عشر: منظومة القيم والأخلاق والسلوكيات

١. يقوم المجلس بتفويض لجنة حاكمية تكنولوجيا المعلومات باعتماد 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.

٢. 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 Framework) (ITAF) الصادر عن جمعية التدقيق والرقابة على نظم المعلومات (ISACA) وتحديثاته.

٣. 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.