دليل حاكمية وادارة المعلومات والتكنولوجيا المصاحبة لها

البنك الاستثماري

(نسخة محدثة بتاريخ 6 شباط 2020)

قائمة المحتويات

المقدمة

يسعى البنك الاستثماري للاسترشاد بمبادئ حاكمية تكنولوجيا المعلومات كونها تساعد البنك على تحقيق أهدافه في مجالات حوكمة تقنية المعلومات المؤسسية وادارتها بالإضافة إلى أنها تساعد على ايجاد القيمة القصوى من تقنية المعلومات من خلال المحافظة على الاتزان المعقول بين تحقيق الفوائد وتقليل مستويات المخاطر.

ان البنك الاستثماري ومن خلال هذا الدليل يأكد على ضرورة العمل بموجبه للنهوض بالأداء، حيث يتكون الدليل من مجموعة من المرتكزات والمبادئ الاساسية، أولها التوافق الاستراتيجي المطلوب تحقيقه من خلال الاهداف الاستراتيجية لتكنولوجيا المعلومات والتي بدورها تساهم في تحقيق الاهداف الاستراتيجية للبنك.

الهدف من الدليل

تم إعداد هذا الدليل للانسجام مع تعليمات حاكمية وادارة المعلومات والتكنولوجيا المصاحبة لها الصادرة عن البنك المركزي الأردني والتعليمات والقوانين الصادرة من قبل الجهات الرقابية المنظمة لأعمال البنك، بالإضافة الى الأهداف التي تم ذكرها في المقدمة أعلاه.

الاختصارات

APO: Align, Plan, Organize.

CGEIT: Certified in the Governance of Enterprise IT.

CISA: Certified Information System Auditor.

COBIT: Control Objective for Information and Related Technologies.

DSS: Delivery, Service, Support.

EDM: Evaluate, Direct, Monitor.

IEC: International Electro Technical Commission.

ISACA: Information System Audit and Control Association.

ISO: International Organization for standardization.

ITAF: Information Technology Assurance Framework.

ITIL: Information Technology Infrastructure Library.

PCI: Payment Card Industry.

RACI Chart: Responsible, Accountable, Consulted, Informed Chart.

ROI: Return on Investment.

تعريفات عامة

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

1. البنك: البنك الاستثماري.
2. المجلس: مجلس إدارة البنك الاستثماري.
3. أعضاء المجلس: أعضاء مجلس إدارة البنك الاستثماري (سواء بصفتهم الشخصية أو ممثلين لشخص اعتباري) بما فيهم رئيس ونائب رئيس المجلس.
4. البنك المركزي: البنك المركزي الأردني.
5. حاكمية المعلومات والتكنولوجيا المصاحبة لها: توزيع الأدوار والمسؤوليات وتوصيف العلاقات بين الاطراف والجهات المختلفة وأصحاب المصالح (مثل المجلس والادارة التنفيذية) بهدف تعظيم القيمة المضافة للمؤسسة باتباع النهج الأمثل الذي يكفل الموازنة بين المخاطر والعوائد المتوقعة، من خلال اعتماد القواعد والاسس والآليات اللازمة لصنع القرار وتحديد التوجهات الاستراتيجية والأهداف في البنك وآليات مراقبة وفحص امتثال مدى تحققها بما يكفل ديمومة وتطور البنك.
6. ادارة المعلومات والتكنولوجيا المصاحبة لها: مجموعة النشاطات المستمرة التي تقع ضمن مسؤولية الادارة التنفيذية وتشمل التخطيط بغرض تحقيق الاهداف 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 اهداف البنك وتوجهاته الاستراتيجية.
7. عمليات حاكمية تكنولوجيا المعلومات: مجموعة الممارسات والنشاطات المنبثقة عن سياسات المؤسسة واللازمة لتحقيق اهداف المعلومات والتكنولوجيا المصاحبة لها.
8. اهداف المعلومات والتكنولوجيا المصاحبة لها: مجموعة الاهداف الرئيسية والفرعية المتعلقة بنشاطات الحاكمية والادارة للمعلومات والتكنولوجيا المصاحبة لها واللازمة لتحقيق الاهداف المؤسسية.
9. الاهداف المؤسسية: مجموعة الاهداف المؤسسية المتعلقة بالحاكمية والادارة المؤسسية واللازمة لتحقيق احتياجات اصحاب المصالح واهداف هذا الدليل.
10. الادارة التنفيذية العليا: تشمل مدير عام البنك والمدير المالي ومدير العمليات ومساعد المدير العام ومدير ادارة المخاطر ومدير الخزينة (الاستثمار) ومدير الامتثال بالإضافة لأي موظف في البنك له سلطة تنفيذية موازية لأي من سلطات اي من المذكورين ويرتبط وظيفياً مباشرةً بالمدير العام.

11. اصحاب المصالح (Stakeholders): أي ذي مصلحة في البنك مثل المساهمين أو الموظفين أو الدائنين أو العملاء أو المزودين الخارجيين أو الجهات الرقابية المعنية.
12. On – Site: مكان العملية في نفس بناية الادارة العامة للبنك في الاردن.
13. Off – Site: مكان العملية في بناية مغايرة لبناية الادارة العامة للبنك في الاردن لكن بنفس المحافظة.
14. Near – Site: مكان العملية في محافظة مغايرة للمحافظة التي تتواجد فيها الادارة العامة للبنك في الاردن.
15. Off – shore: مكان العملية في بلد مغاير لبلد الادارة العامة للبنك.
16. 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 ادارة البنك لتحقيق تلك المتطلبات لفترة لا تقل عن 3 سنوات متتالية ولا تزيد عن 6 سنوات متتالية.

الفصل الاول: أهداف حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها

تهدف حاكمية وادارة المعلومات والتكنولوجيا المصاحبة الى ما يلي:

1. تلبية احتياجات أصحاب المصالح (Stakeholders' 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. ادارة حصيفة لموارد ومشاريع تكنولوجيا المعلومات، تعظم الاستفادة من تلك الموارد وتقلل الهدر منها.
   ج. توفير بنية تحتية تكنولوجية متميزة وداعمة تمكن البنك من تحقيق أهدافه.
   د. الارتقاء بعمليات البنك المختلفة من خلال توظيف منظومة تكنولوجية كفؤة وذات اعتمادية متميزة.
   ه. إدارة حصيفة لمخاطر تكنولوجيا المعلومات تكفل الأمن والحماية اللازمة لموجودات البنك.
   و. المساعدة في تحقيق الامتثال لمتطلبات القوانين والتشريعات والتعليمات بالإضافة للامتثال لاستراتيجية وسياسات واجراءات 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 الاطراف الخارجية الموكل إليها تنفيذ عمليات ومهام وخدمات ومنتجات.
2. تحقيق الشمولية في حاكمية وادارة المعلومات والتكنولوجيا المصاحبة لها من حيث الاخذ بالاعتبار ليس فقط التكنولوجيا بحد ذاتها وإنما توفير عناصر تمكين (دعامات) سبعة (7 Enablers/Components) تكون مصاحبة ومكملة لخدمات تكنولوجيا المعلومات تتمثل بـ:
   أ. المبادئ والسياسات وأطر العمل.
   ب. عمليات حاكمية تكنولوجيا المعلومات.
   ج. الهياكل التنظيمية.
   د. المعلومات والتقارير.
   ه. الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات.
   و. المعارف والمهارات والخبرات.
   ز. منظومة القيم والاخلاق والسلوكيات وضرورة توفيرها بمواصفات وابعاد محددة لتحقيق وخدمة متطلبات واهداف المعلومات والتكنولوجيا المصاحبة لها ليس فقط في عمليات تكنولوجيا المعلومات وحسب وانما في كافة عمليات البنك المرتكزة على المعلومات والتكنولوجيا.

3. تبني ممارسات وقواعد العمل والتنظيم بحسب أفضل المعايير الدولية كنقطة انطلاق يتم الارتكاز والبناء عليها في مجالي حاكمية وإدارة عمليات ومشاريع وموارد تكنولوجيا المعلومات.
4. فصل عمليات ومهام ومسؤوليات المجلس في مجال الحاكمية عن تلك التي تقع ضمن حدود مسؤولية الادارة التنفيذية بخصوص المعلومات والتكنولوجيا المصاحبة لها.
5. تعزيز آليات الرقابة الذاتية والرقابة المستقلة وفحص الامتثال في مجالي حاكمية وادارة المعلومات والتكنولوجيا المصاحبة لها وبما يسهم في تحسين وتطوير الاداء بشكل مستمر.

- **نطاق وآلية التطبيق والاطراف المعنية:**

على البنك، عند توقيع اتفاقيات إسناد (Outsourcing) مع الغير لتوفير الموارد البشرية والخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات بهدف تسيير عمليات البنك ، التأكد من التزام الغير بتطبيق بنود هذه التعليمات بشكل كلي أو جزئي بالقدر الذي يتناسب مع أهمية وطبيعة عمليات البنك والخدمات والبرامج والبنية التحتية المقدمة قبل واثناء فترة التعاقد ، وبما لا يعفي المجلس والادارة التنفيذية العليا من المسؤولية النهائية لتحقيق متطلبات تعليمات البنك المركزي الأردني حول حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها بما في ذلك متطلبات التدقيق الواردة ضمن نفس التعليمات.

يشمل نطاق تطبيق الدليل كافة عمليات البنك المرتكزة على تكنولوجيا المعلومات بمختلف الفروع والادارات، وتعتبر جميع الاطراف (اصحاب المصالح) معنية بتطبيق الدليل كل بحسب دوره وموقعه، ولتسهيل علمية التطبيق يتم البدء من خلال مشروع / برنامج (مجموعة مشاريع ذات صلة) يدار من قبل البنك لإيجاد وتوفير البيئة اللازمة وتحقيق متطلبات الدليل، وعلى وجه التحديد الاطراف التالية ومسؤولياتها الرئيسية بهذا الخصوص:

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

2. المدير العام ونوابه ومساعديه ومدراء العمليات والفروع: تولي مسؤوليات تسمية الاشخاص المناسبين من ذوي الخبرة بعمليات البنك لتمثيلهم في المشروع وتوصيف مهامهم ومسؤولياتهم.

3. مدير ولجان تكنولوجيا المعلومات التوجيهية ومدراء المشاريع: تولي مسؤوليات ادارة المشروع /البرنامج وتوجيهه والاشراف عليه بشكل مباشر والتوصية بتوفير الموارد اللازمة لإتمامه، والتأكد من الفهم الصحيح من قبل كافة الاطراف بمتطلبات وأهداف الدليل.

4. التدقيق الداخلي: تولي مسؤولياته المناطة به بموجب التعليمات بشكل مباشر، والمشاركة في المشروع / البرنامج بما يمثل دور التدقيق الداخلي في الامور التنفيذية كمستشار ومراقب مستقل لتسهيل وانجاح اتمام المشروع / البرنامج.

5. ادارات المخاطر وأمن المعلومات والامتثال والقانونية: تولي المسؤوليات المشاركة في المشروع / البرنامج بما يمثل دور تلك الادارات، والتأكد من تمثيل المشروع / البرنامج من قبل كافة الاطراف المعنية.

6. المتخصصين وحملة الشهادات الفنية والمهنية الخاصة بالمعيار(CGEIT، COBIT 2019 Foundation, COBIT 2019 Design and Implementation,) والمستعان بهم من داخل البنك ومن خارجه، تولي دور المرشد لنشر المعرفة بالمعيار وتسهيل عملية التطبيق.

تعتبر متطلبات هذا الدليل بعد تطبيقه خطوة اولى ونقطة بداية تجاه التطوير والتحسين المستمرين لحاكمية وادارة المعلومات والتكنولوجيا المصاحبة لها، وعليه يتوجب على البنك مواكبة الاصدارات الناشئة المستقبلية وتحديثاتها فيما يخص الإطار العام الذي تم الاستناد له عند صياغة هذا الدليل ومعايير (COBIT) وما يحتويه من معايير دولية اخرى مستند لها ضمن هذا الإطار.

الفصل الثاني: لجان حاكمية وادارة المعلومات والتكنولوجيا المصاحبة لها

أولى البنك الاستثماري عناية خاصة للعملية التخطيطية والبرامج التنفيذية والنظم الإشرافية باعتبارها القواعد الحاكمة لأي سياسات تتعلق بنفقاتها وايراداتها شكلاً ومضمونا وصولا لتحقيق النتائج الجيدة وبما يساعد على تقليل المخاطر الى حدها الادنى حتى لو تعذر عمليا تجنب تلك المخاطر بشكل كامل.

ومن المهم دائما رصد تلك المخاطر وتحديدها للتعامل معها وفق عملية إدارية علمية وفعالة وشفافة من خلال سياسات متجددة واجراءات متطورة وأنظمة تساعد على الكشف المبكر عن تلك المخاطر والتعامل معها ومواجهتها أولا بأول.

وبالتأكيد فان نجاح تلك السياسات والاجراءات والانظمة يتطلب التزام جميع الموظفين بها وتفهمها، وبعكس ذلك فان فعاليتها تصبح عديمة الجدوى أو الفائدة، الامر الذي يستدعي ان تكون منظمة بشكل واضح وبسيط وفعال ومفهوم ليكون جميع الموظفين قادرين على التعامل معها وتنفيذها بسرعة ودقة.

ومن اجل هذه الغاية وحتى يتمكن مجلس الادارة من تغطية ومتابعة المخاطر التي يمكن ان يتعرض لها البنك بطريقة عملية، فقد قام بتشكيل اللجان التي تقوم برفع تقارير دورية للمجلس ككل تتضمن مراجعة للمخاطر القائمة والمستجدة، وفق المهام والمسؤوليات المنوطة بكل منها، لمساعدة مجلس الادارة على الاحاطة بكافة الانشطة ذات الصلة بمهام هذه اللجان بصورة سليمة.

أولاً: لجنة حاكمية تكنولوجيا المعلومات:

تتشكل هذه اللجنة من ثلاثة أعضاء من مجلس الإدارة على الأقل ، ويفضل أن تضم في عضويتها أشخاص من ذوي الخبرة أو المعرفة الاستراتيجية في تكنولوجيا المعلومات، وللجنة الاستعانة عند اللزوم وعلى نفقة البنك بخبراء خارجيين وذلك بالتنسيق مع رئيس المجلس بغرض تعويض النقص بهذا المجال من جهة ولتعزيز الرأي الموضوعي من جهة أخرى ، وللجنة دعوة أي من إداري البنك لحضور اجتماعاتها للاستعانة برأيهم بما فيهم المعنيين في التدقيق الداخلي واعضاء الادارة التنفيذية العليا أو المعنيين في التدقيق الخارجي ، ويحدد المجلس أهدافها ويفوضها بصلاحيات من قبله وذلك وفق ميثاق يوضح ذلك، وعلى أن تقوم برفع تقارير دورية للمجلس، علما بأن تفويض المجلس صلاحيات للجنة أو أي لجنة أخرى لا يعفيه ككل من تحمل مسؤولياته بهذا الخصوص، وتجتمع اللجنة بشكل ربع سنوي على الأقل، وتحتفظ بمحاضر اجتماعات موثقة وتتولى المهام التالية:

1. اعتماد الأهداف والخطة الاستراتيجية لتكنولوجيا المعلومات.
2. اعتماد الهياكل 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.
3. استخدام الأدوات والمعايير اللازمة لمراقبة والتأكد من مدى تحقق الأهداف الاستراتيجية للبنك، 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.

4. اعتماد الإطار العام لإدارة وضبط ومراقبة موارد ومشاريع تكنولوجيا المعلومات يحاكي أفضل الممارسات الدولية المقبولة بهذا الخصوص وعلى وجه التحديد (COBIT – Control Objective for Information and Related Technology) يتوافق ويلبي تحقيق أهداف ومتطلبات تعليمات البنك المركزي.
5. اعتماد مصفوفة الأهداف المؤسسية بشكل مستدام الواردة في الملحق رقم 1 وأهداف المعلومات والتكنولوجيا المصاحبة لها الواردة في الملحق رقم 2 وتوصيف الأهداف الفرعية اللازمة لتحقيقها.
6. اعتماد مصفوفة للمسؤوليات (RACI Chart) اتجاه العمليات الرئيسية لحاكمية تكنولوجيا المعلومات الواردة في الملحق رقم 3 والعمليات الفرعية المنبثقة عنها.
7. 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 عمليات حاكمية تكنولوجيا المعلومات الواردة في الملحق رقم 3.
8. اعتماد موازنة موارد ومشاريع تكنولوجيا المعلومات بما يتوافق والأهداف الاستراتيجية للبنك.
9. الاشراف العام والاطلاع على سير عمليات وموارد ومشاريع تكنولوجيا المعلومات للتأكد من كفايتها ومساهمتها الفاعلة في تحقيق متطلبات وأعمال البنك.
10. الاطلاع على تقارير التدقيق لتكنولوجيا المعلومات واتخاذ ما يلزم من اجراءات لمعالجة الانحرافات.
11. يسمح باعتماد تقارير المدقق الداخلي والخارجي من قبل لجنة حاكمية تكنولوجيا المعلومات أو اللجنة القائمة مقامها وعلى ان يتم اطلاع المجلس على تلك التقارير.
12. التوصية للمجلس باتخاذ الاجراءات اللازمة لتصحيح أية انحرافات.
13. التوصية للمجلس فيما يخص مشتريات دائرة تكنولوجيا المعلومات للنفقات الرأسمالية و/أو التشغيلية التي تتجاوز صلاحيات الإدارة التنفيذية.
14. اعتماد أهمية وترتيب أولوية الأهداف (Governance and Management Objectives) ومدى ارتباطها بباقي عناصر التمكين (Enablers or Components) وذلك بناء على دراسة نوعية و/أو كمية تعد لهذا الغرض بشكل سنوي على الأقل تأخذ بعين الاعتبار الـ (Design Factors) الواردة في (COBIT 2019 – Design Guide).

ثانياً: اللجنة التوجيهية لتكنولوجيا المعلومات (IT Steering Committee):

على الإدارة التنفيذية العليا تشكيل اللجان التوجيهية اللازمة لضمان عملية التوافق الاستراتيجي لتكنولوجيا المعلومات لتحقيق الاهداف الاستراتيجية للبنك وبشكل مستدام ، وعليه يتم تشكيل لجنة تسمى باللجنة التوجيهية لتكنولوجيا المعلومات

برئاسة المدير العام وعضوية مدراء الادارة التنفيذية العليا بما في ذلك مدير تكنولوجيا المعلومات ومدير إدارة المخاطر ومدير أمن المعلومات وينتخب المجلس أحد أعضائه ليكون عضواً مراقباً في هذه اللجنة بالإضافة لمدير التدقيق الداخلي ، ويمكنها دعوة الغير لدى الحاجة لحضور اجتماعاتها ، وتوثق اللجنة اجتماعاتها بمحاضر اصولية، على أن تكون دورية الاجتماعات مرة كل ثلاثة أشهر على الاقل ، وتتولى على وجه الخصوص القيام بالمهام التالية:

1. وضع الخطط السنوية الكفيلة بالوصول للأهداف الاستراتيجية المقرة من قبل المجلس، والاشراف على تنفيذها لضمان تحقيقها ومراقبة العوامل الداخلية والخارجية المؤثرة عليها بشكل مستمر.
2. ربط مصفوفة الاهداف المؤسسية بمصفوفة أهداف المعلومات والتكنولوجيا المصاحبة لها واعتمادها ومراجعتها بشكل مستمر وبما يضمن تحقيق الاهداف الاستراتيجية للبنك وأهداف الدليل، ومراعاة تعريف مجموعة معايير للقياس ومراجعتها وتكليف المعنيين من الادارة التنفيذية بمراقبتها بشكل مستمر واطلاع اللجنة على ذلك.
3. التوصية بتخصيص الموارد المالية وغير المالية اللازمة لتحقيق الاهداف وعمليات حاكمية تكنولوجيا المعلومات، والاستعانة بالعنصر البشري الكفوء والمناسب في المكان المناسب من خلال هياكل تنظيمية تشمل كافة العمليات اللازمة لدعم الاهداف تراعي فصل المهام وعدم تضارب المصالح، وتطويع البنية التحتية التكنولوجية والخدمات الاخرى المتعلقة بها خدمة للأهداف وتولي عمليات الاشراف على سير تنفيذ مشاريع وعمليات حاكمية تكنولوجيا المعلومات.
4. ترتيب مشاريع وبرامج تكنولوجيا المعلومات حسب الاولوية.
5. مراقبة مستوى الخدمات الفنية والتكنولوجية والعمل على رفع كفاءتها وتحسينها بشكل مستمر.
6. رفع التوصيات اللازمة للجنة حاكمية تكنولوجيا المعلومات بخصوص الامور التالية:
   أ. تخصيص الموارد اللازمة والآليات الكفيلة بتحقيق مهام لجنة حاكمية تكنولوجيا المعلومات.
   ب. أية انحرافات قد تؤثر سلبا على تحقيق الاهداف الاستراتيجية.
   ج. أية مخاطر غير مقبولة متعلقة بتكنولوجيا المعلومات.
   د. تقارير الأداء والامتثال بمتطلبات الإطار العام لإدارة وضبط ومراقبة موارد ومشاريع تكنولوجيا المعلومات.
7. تزويد لجنة حاكمية تكنولوجيا المعلومات بمحاضر اجتماعاتها اولا بأول والحصول على ما يفيد الاطلاع عليها.
8. مراجعة المخاطر الخاصة بإدارة المعلومات والتكنولوجيا المصاحبة لها بما في ذلك المخاطر التي تم تنسيبها من قبل اللجنة التوجيهية لأمن المعلومات ورفع التوصيات للجان المعنية.

الفصل الثالث: أهداف الحاكمية والادارة

1. تعتبر أهداف الحاكمية والادارة حداً أدنى يتوجب على ادارة البنك العليا الامتثال لها وتحقيقها بشكل مستمر، وتعتبر اللجنة التوجيهية لتكنولوجيا المعلومات المسؤول الأول عن ضمان الامتثال بتحقيق متطلباتها، ولجنة حاكمية تكنولوجيا المعلومات والمجلس ككل المسؤول النهائي بهذا الخصوص، ويتوجب على كافة دوائر البنك وعلى وجه الخصوص دائرة تكنولوجيا المعلومات وإدارة أمن المعلومات وإدارة المشاريع تحديد عملياتها وإعادة صياغتها بحيث تحاكي وتغطي متطلبات كافة عمليات حاكمية تكنولوجيا المعلومات.
2. يتولى المجلس المسؤولية المباشرة لعمليات التقييم والتوجيه والرقابة (EDM).
3. يتولى المجلس ودائرة إدارة المخاطر المسؤولية المباشرة عن عملية ضمان ادارة حصيفة لمخاطر تكنولوجيا المعلومات وعملية ادارة المخاطر.

الفصل الرابع: التدقيق الداخلي والخارجي

1. 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 وادارة موارد ومشاريع تكنولوجيا المعلومات وعمليات البنك المرتكزة عليها مراجعة فنية متخصصة (IT Audit) ، من خلال كوادر مهنية ومؤهلة ومعتمدة دوليا بهذا المجال ، حاصلين على شهادات اعتماد مهنية سارية مثل (CISA) من جمعيات دولية مؤهلة بموجب معايير الاعتماد الدولي للمؤسسات المانحة للشهادات المهنية (ISO/IEC 17024) و/أو أية معايير اخرى موازية.
2. على لجنة التدقيق المنبثقة عن المجلس من جهة والمدقق الخارجي من جهة اخرى تزويد البنك المركزي الاردني بتقرير سنوي للتدقيق الداخلي وآخر للتدقيق الخارجي على التوالي يتضمن رد الادارة التنفيذية واطلاع وتوصيات المجلس بخصوصه، وذلك وفق نموذج تقرير تدقيق (مخاطر – ضوابط) المعلومات والتكنولوجيا المصاحبة لها 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 اخرى.
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 الالتزام بما يلي:

أ. معايير تدقيق تكنولوجيا المعلومات بحسب آخر تحديث للمعيار الدولي ITAF)) الصادر عن جمعية التدقيق والرقابة على نظم المعلومات (ISACA) ومنها:

- ✓ تنفيذ مهمات التدقيق ضمن خطة معتمدة بهذا الخصوص تأخذ بعين الاعتبار الاهمية 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 والادارية (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 الاخرى (المالية والتشغيلية والقانونية)، والقدرة على تقديم الدليل (Evidence) المتناسب مع الحالة، والحس العام في كشف الممارسات غير المقبولة والمخالفة لأحكام القوانين والانظمة والتعليمات.

ب. فحص وتقييم ومراجعة عمليات توظيف وادارة موارد تكنولوجيا المعلومات وعمليات البنك المرتكزة عليها واعطاء رأي عام (Reasonable Overall Audit Assurance) حيال مستوى المخاطر الكلي للمعلومات والتكنولوجيا المصاحبة لها ضمن برنامج تدقيق ، على أن يكون تكرار التدقيق لكافة المحاور أو جزء منها كحد ادنى مرة واحدة سنوياً على الأقل في حال تم تقييم المخاطر بدرجة (5 أو 4) بحسب سلم تقييم المخاطر ومرة واحدة كل سنتين على الاقل في حال تم تقييم المخاطر بدرجة (3) ، ومرة واحدة كل ثلاث سنوات على الاقل في حال تم تقييم المخاطر بدرجة (2 أو 1) ، مع مراعاة التغيير المستمر في مستوى المخاطر والاخذ بعين الاعتبار التغييرات الجوهرية التي تطرأ على بيئة المعلومات والتكنولوجيا المصاحبة لها خلال فترات التدقيق المذكورة ، على ان يتم تزويد البنك المركزي بتقارير التدقيق لأول مرة بغض النظر عن درجة تقييم المخاطر ، وعلى ان تشمل عمليات التقييم للمحاور المذكورة آليات البنك المتبعة من حيث التخطيط الاستراتيجي ورسم السياسات والمبادئ واجراءات العمل المكتوبة والمعتمدة وآليات توظيف الموارد المختلفة بما فيها موارد تكنولوجيا المعلومات والعنصر البشري، وآليات وأدوات المراقبة والتحسين والتطوير والعمل على توثيق نتائج التدقيق وتقييمها اعتمادا على اهمية الاختلالات ونقاط الضعف (الملاحظات) بالإضافة للضوابط المفعلة وتقييم مستوى المخاطر المتبقية والمتعلقة بكل منها باستخدام معيار منهجي لتحليل وقياس المخاطر، متضمنا الاجراءات التصحيحية المتفق عليها والمنوي اتباعها من قبل ادارة

البنك بتواريخ محددة للتصحيح ، مع الاشارة ضمن جدول خاص الى رتبة صاحب المسؤولية في البنك مالك كل ملاحظة.

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

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

5. من الممكن اسناد (Outsource) دور المدقق الداخلي للمعلومات والتكنولوجيا المصاحبة لها (Internal IT Audit) لجهة خارجية متخصصة مستقلة تماما عن المدقق الخارجي المعتمد بهذا الخصوص شريطة تلبية كافة متطلبات هذا الدليل او اي سياسات اخرى ذات صلة واحتفاظ لجنة التدقيق المنبثقة عن المجلس والمجلس نفسه بدورهما فيما يتعلق بفحص الامتثال والتأكد من تلبية هذه المتطلبات كحد أدنى.

الفصل الخامس: المبادئ والسياسات وأطر العمل

1. على المجلس أو من يفوض من لجانه اعتماد منظومة المبادئ والسياسات وأطر العمل (Frameworks) وعناصر تصميم نظام الحاكمية (Design Factor) و (Focus Areas) اللازمة لتحقيق الإطار العام لإدارة وضبط ومراقبة موارد ومشاريع تكنولوجيا المعلومات وبما يلبي متطلبات الأهداف وعمليات حاكمية تكنولوجيا المعلومات.
2. على المجلس أو 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 عمليات حاكمية تكنولوجيا المعلومات.
3. على المجلس أو من يفوض من لجانه اعتماد منظومة السياسات اللازمة لإدارة موارد وعمليات حاكمية تكنولوجيا المعلومات، واعتبار منظومة السياسات هذه حداً أدنى مع إمكانية الجمع والدمج لتلك السياسات حسب ما تقتضيه طبيعة العمل، وعلى أن يتم تطوير سياسات أخرى ناظمة مواكبة لتطور أهداف البنك وآليات العمل، وعلى أن تحدد كل سياسة الجهة المالكة ونطاق التطبيق ودورية المراجعة والتحديث وصلاحيات الاطلاع والتوزيع والأهداف والمسؤوليات واجراءات العمل المتعلقة بها، والعقوبات في حالة عدم الامتثال وآليات فحص الامتثال.
4. يراعى لدى انشاء السياسات مساهمة كافة الشركاء الداخليين والخارجيين واعتماد أفضل الممارسات الدولية وتحديثاتها كمراجع لصياغة تلك السياسات مثل:

COBIT 2019, ISO/IEC 27001/2, ISO 31000, ISO/IEC 38500, ISO/IEC 9126, ISO/IEC 15504, ISO 22301, PCI DSS, ITIL,… etc.

الفصل السادس: الهياكل التنظيمية
1. على المجلس اعتماد الهياكل التنظيمية (الهرمية واللجان) وعلى وجه الخصوص تلك المتعلقة بإدارة موارد وعمليات ومشاريع تكنولوجيا المعلومات، وادارة مخاطر تكنولوجيا المعلومات، وادارة أمن المعلومات، وادارة الموارد البشرية وتحقيق أهداف البنك بكفاءة وفعالية. 2. يراعى ضمان فصل المهام المتعارضة بطبيعتها ومتطلبات الحماية التنظيمية المتعلقة بالرقابة الثنائية كحد أدنى وكفاية وتحديث الوصف الوظيفي لدى اعتماد وتعديل الهياكل التنظيمية للبنك.
الفصل السابع: المعلومات والتقارير
1. 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 Currency) ومتطلبات السرية بحسب سياسة تصنيف البيانات ومتطلبات التوافرية والامتثال بتلك المعلومات والتقارير ، بالإضافة للمتطلبات الاخرى الواردة في المعيار (COBIT 2019 – Enabling Information) والمتمثلة بالـ (Objectivity, Believability, Reputation, Relevancy, Appropriate Amount, Concise Representation, Consistent Representation, Interpretability, Understandability, Ease of Manipulation, Restricted Access). 2. على المجلس أو من يفوض من لجانه اعتماد منظومة المعلومات والتقارير، 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.

الفصل الثامن: الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات
1. على المجلس او من يفوض من لجانه والادارة التنفيذية العليا اعتماد منظومة الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات الداعمة والمساعدة لتحقيق عمليات حاكمية تكنولوجيا المعلومات وبالتالي أهداف المعلومات وتكنولوجيا المصاحبة لها، وبالتالي الاهداف المؤسسية. 2. على المجلس او من يفوض من لجانه والادارة التنفيذية العليا اعتماد منظومة الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات، وعلى ان يتم توفيرها وتطويرها بشكل مستمر لمواكبة تطور اهداف وعمليات البنك وبما يتفق وأفضل الممارسات الدولية المقبولة بهذا الخصوص.
الفصل التاسع: المعارف والمهارات والخبرات
1. على المجلس أو من يفوض من لجانه اعتماد مصفوفة المؤهلات (HR Competencies) وسياسات ادارة الموارد البشرية اللازمة لتحقيق متطلبات عمليات حاكمية تكنولوجيا المعلومات، وضمان وضع الرجل المناسب في المكان المناسب. 2. على ادارة البنك توظيف العنصر البشري المؤهل والمدرب من الاشخاص ذوي الخبرة في مجالات ادارة موارد تكنولوجيا المعلومات وادارة المخاطر وادارة امن المعلومات وادارة تدقيق تكنولوجيا المعلومات اعتمادا على معايير المعرفة الاكاديمية والمهنية والخبرة العملية باعتراف جمعيات دولية مؤهلة بموجب معايير الاعتماد الدولي للمؤسسات المانحة للشهادات المهنية (ISO/IEC 17024) و/أو اية معايير اخرى موازية كل بحسب اختصاصه، على ان يتم اعادة تأهيل وتدريب الكوادر الموظفة حاليا لتلبية المتطلبات. 3. على الادارة التنفيذية في البنك الاستمرار برفد موظفيها ببرامج التدريب والتعليم المستمر للحفاظ على مستوى من المعارف والمهارات يلبي ويحقق عمليات حاكمية تكنولوجيا المعلومات. 4. على الادارة التنفيذية في البنك تضمين آليات التقييم السنوي (Performance Evaluation) للكوادر بمعايير قياس موضوعية تأخذ بعين الاعتبار المساهمة من خلال المركز الوظيفي بتحقيق اهداف البنك.

الفصل العاشر: منظومة القيم والاخلاق والسلوكيات

1. على المجلس أو من يفوض من لجانه اعتماد 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.
2. على المدقق الداخلي والمدقق الخارجي الامتثال لمنظومة الاخلاق والممارسات المهنية المعتمدة من قبل المجلس بحيث تتضمن بالحد الادنى منظومة الاخلاق المهنية الواردة في المعيار الدولي (ITAF) الصادر عن جمعية التدقيق والرقابة على نظم المعلومات (ISACA) وتحديثاته.
3. على المجلس والادارة التنفيذية العليا توظيف الاليات المختلفة لتشجيع تطبيق السلوكيات المرغوبة وتجنب السلوكيات غير المرغوبة من خلال اتباع اساليب الحوافز والعقوبات على سبيل المثال لا الحصر.

احكام ختامية

1. يُعمل بهذا الدليل اعتبارا من تاريخ إقراره وتُلغى كافة السياسات والتعليمات السابقة المتعلقة بهذا الخصوص.
2. يخضع هذا الدليل للمراجعة مرة واحدة كل عامين كحد أدنى أو كلما دعت الحاجة لذلك.
3. يلتزم البنك بالامتثال لدليل الحاكمية المؤسسية الخاص به ضمن الفترات المحددة من قبل البنك المركزي بموجب تعليمات الحاكمية المؤسسية سارية المفعول، وتعليمات حاكمية وادارة المعلومات والتكنولوجيا المصاحبة لها سارية المفعول وأي تعليمات أخرى لاحقة.
4. يلتزم البنك بنشر الدليل الخاص به على موقعه الإلكتروني، وبأي طريقة أخرى لإعلام الجمهور، بالإضافة الى الإفصاح في التقرير السنوي عن وجود دليل خاص لحاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها او متضمن لدليل الحاكمية المؤسسية لدى البنك، والافصاح أيضاً عن المعلومات التي تهم اصحاب المصالح بما فيها الدليل ومدى الالتزام بما جاء فيه.

المراجع

- تعليمات الحاكمية المؤسسية للبنوك الصادرة عن البنك المركزي الأردني سارية المفعول.
- تعليمات حاكمية وادارة المعلومات والتكنولوجيا المصاحبة لها سارية المفعول والتعاميم ذات العلاقة.
- تعتبر الوثائق التالية جزء لا يتجزأ من الدليل وتقرأ إلى جانبها كوحدة واحدة:
  أ. وثيقة تصميم نظام حاكمية تكنولوجيا المعلومات
  ب. وثيقة تطبيق نظام حاكمية تكنولوجيا المعلومات