دليل حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها

الفهرس

المقدمة

إنطلاقاً من حرص البنك التجاري الاردني على سلامة أوضاعه واتباع أفضل الممارسات الدولية في مجال إدارة موارد ومشاريع وخدمات تكنولوجيا المعلومات بالشكل الذي يمكنه من تسيير أعماله وتحقيق أهدافه الاستراتيجية بفاعلية وكفاءة عالية والذي بدوره ينعكس بشكل إيجابي على جودة منتجات وخدمات البنك من جهة وعلى آليات صنع القرار وإدارة المخاطر من جهة آخرى، وكذلك إحتراماً لسلامة الجهاز المصرفي ككل وإلتزاماً بالمعايير الدولية للممارسات المصرفية السليمة، يدرك البنك أنه يقتضي الإلتزام بأفضل المعايير في مجال المعلومات والتكنولوجيا المصاحبة لها.

وقد أدرك مجلس الإدارة والادارة التنفيذية الحاجة إلى تبني المنتجات الناجحه والتي تستوجب تطبيق تقنية المعلومات بشكل كفوء وفعال جنباً إلى جنب مع مختلف ممارسات وإجراءات العمل لدى البنك وبالشكل الذي يستدعي وجود اطار ومبادئ حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها، ففصل عمليات ومهام ومسؤوليات المجلس في مجال الحاكمية عن تلك التي تقع ضمن حدود مسؤولية الإدارة التنفيذية بخصوص المعلومات والتكنولوجيا المصاحبة لها وإتباع المرتكزات والمعايير السليمة في إدارة موارد تكنولوجيا المعلومات بحسب الممارسات الدولية الفضلى وعلى رأسها إطار (COBIT) لضبط المخاطر والوصول لتطلعات أصحاب المصالح بتطبيق قواعد الحاكمية السليمة، وتجنباً للدخول في استثمارات غير مجدية ومصاريف غير مبررة تترجم الى خسائر طائلة والتي قد تنال في بعض الاحيان من سمعة البنك وإداؤه .

هذا وللتأكيد على الهوية الخاصّة بالبنك التجاري الأردني فقد تم إعداد هذه الدليل وإرفاقه بدليل حاكمية المؤسسة والذي يعبر عن نظرة البنك الخاصّة بحاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها من حيث مفهومها وأهميتها ومبادئها الأساسية وبشكل يراعي التشريعات وأفضل الممارسات الدولية ويؤكد على إلتزام البنك بكافة القوانين والتشريعات الصادرة بالخصوص.

هذا وتسري أحكام هذا الدليل على فروع البنك التجاري الأردني في الاردن، ويقوم البنك بنشر دليل حاكمية تكنولوجيا المعلومات على الموقع الإلكتروني الخاص في البنك ويلتزم بالإفصاح في تقريره السنوي عن الدليل ومدى التزامه بتطبيق ما جاء فيه.

الباب الأول: حاكمية تكنولوجيا المعلومات ونطاقها وأهدافها

أولاً: الحاكمية :

تعتبر إدارة المعلومات والتكنولوجيا المصاحبة لها بأنها مجموعة من 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 وتوصيل الخدمات والدعم، ونشاطات المراقبة كالقياس والتقييم، وبالشكل الذي يكفل ديمومة تحقيق أهداف البنك وتوجهاته الاستراتيجية، وفي ضوء ذلك تعرف حاكمية المعلومات والتكنولوجيا المصاحبة لها بعملية توزيع الأدوار والمسؤوليات وتوصيف العلاقات بين الأطراف والجهات المختلفة وأصحاب المصالح بهدف تعظيم القيمة المضافة للبنك باتباع النهج الأمثل الذي يكفل الموازنه بين المخاطر والعوائد المتوقعة، ومن خلال اعتماد القواعد والأسس والآليات اللازمة لصنع القرار وتحديد التوجهات الاستراتيجية والأهداف في البنك وآليات مراقبة وفحص مدى الامتثال لتحقيقها سعياً للتقدم والتطور المستمر، وذلك من خلال حاكمية العمليات والتي ترتبط بمجموعة الممارسات والنشاطات المنبثقة عن سياسات البنك واللازمة لتحقيق أهداف المعلومات والتكنولوجيا المصاحبة لها. وتنقسم هذه الاهداف والمنبثقة من الاهداف المؤسسية الى أهداف رئيسية وأهداف فرعية، واللازمة لتلبية احتياجات أصحاب المصالح.

علماً بأن المقصود بأصحاب المصالح أي شخص ذو مصلحة في البنك كالمساهمين أو الموظفين أو الدائنين أو العملاء أو المزودين الخارجيين أو الجهات الرقابية ذات العلاقة بنشاط البنك.

ثانياً: نطاق حاكمية تكنولوجيا المعلومات والأطراف المعنية:

يشمل نطاق تطبيق تعليمات حاكمية تكنولوجيا المعلومات كافة عمليات البنك المرتكزة على تكنولوجيا المعلومات بمختلف الفروع والإدارات، وتعتبر جميع الأطراف أصحاب المصالح معنية بالتطبيق، وقد قام البنك بإطلاق مشروع لإيجاد وتوفير البيئة اللازمة وتحقيق متطلبات تعليمات حاكمية تكنولوجيا المعلومات وفقاً لإطار (COBIT)، ووجود ادوار لكل من :

- الرئيس وأعضاء المجلس والخبراء الخارجيين وذلك لغايات التوجيه العام للمشروع والموافقة على المهام والمسؤوليات وتقديم الدعم والموافقة على التمويل اللازم.
- المدير العام ونوابه ومساعديه ومدراء العمليات لتسمية الاشخاص المناسبين من ذوي الخبرة بعمليات البنك لتمثيلهم في المشروع وتوصيف مهامهم ومسؤولياتهم.
- مدير ولجان تكنولوجيا المعلومات التوجيهية ومدراء المشاريع وذلك لغايات التوجيه ورفع التقارير اللازمة للجنة حاكمية تكنولوجيا المعلومات والأمن السيبراني لمجلس الإدارة ومتابعة الدور المناط بمدراء المشاريع ومراعاة توفر الموارد الكافية والإدراك السليم للأهداف المؤسسية لحاكمية تكنولوجيا المعلومات.

- كما وتناط بالتدقيق الداخلي مهمة تقديم المشورة والمراقبة المستقلة لإنجاح التطبيق وذلك في الأمور التنفيذية كمستشار ومراقب مستقل لتسهيل وإنجاح إتمام إطار التحكم المؤسسي، وذلك من خلال الإطلاع على تقارير التدقيق لتكنولوجيا المعلومات وإتخاذ ما يلزم من إجراءات لمعالجة الإنحرافات ومراقبة مستوى الخدمات الفنية والتكنولوجية والعمل على رفع كفاءتها وتحسينها بشكل مستمر من خلال التوصيات والاقتراحات، وتقوم 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 خلال الربع الاول من كل عام.
- وتلتزم كل من إدارات المخاطر وأمن المعلومات والامتثال والقانونية المشاركة في المشروع بما يمثل دور تلك الإدارات وتطبيق الإطار ومتابعة المتطلبات والإلتزام بالأهداف والسياسات ومن وجود بيئة الرقابة الملائمة.
- ويعتمد البنك على المتخصصين وحملة الشهادات الفنية والمهنية الخاصة بالمعيار (Foundation ,COBIT, COBIT Design and Implementation) من داخل البنك ومن خارجه لتولي دور المرشد والمقيم خلال مراحل التطبيق ولنشر المعرفة بالمعيار وتسهيل عملية الإلتزام.
- ويلتزم البنك عند توقيع اتفاقيات إسناد (Outsourcing) مع الغير لتوفير الموارد البشرية والخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات بهدف تسيير عمليات البنك بالتأكد من إلتزام الغير بتطبيق بنود تعليمات حاكمية تكنولوجيا المعلومات بشكل كلي أو جزئي بالقدر الذي يتناسب مع أهمية وطبيعة عمليات البنك والخدمات والبرامج والبنية التحتية المقدمة قبل وأثناء فترة التعاقد، ولا يعفي المجلس والإدارة التنفيذية العليا من المسؤولية النهائية لتحقيق متطلبات التعليمات مدار البحث بما في ذلك متطلبات التدقيق المشار إليها في هذا الدليل.

ثالثاً: أهداف حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها:

إن الهدف الأساسي لحاكمية تكنولوجيا المعلومات "هو إنشاء القيمة المضافة" للبنك من خلال الاستخدام الامثل لتقنية المعلومات والتكنولوجيا، والحفاظ على القيمة المقدمة بوساطة الإستثمارات الحالية فيها وزيادتها، والتخلص من مبادرات وأصول تقنية المعلومات التي لا تؤدي الى انشاء قيمة مضافة كافية للبنك والذي يعني الاستخدام الأمثل للموارد مع ضبط المخاطر، بالإضافة لمعالجة مخاطر الأعمال المرتبطة بإستخدامات تقنية المعلومات وتملكها وتشغيلها وتبنيها وإدراجها في البنك والتأكد من وجود القدرات الملائمة لتنفيذ الخطة الاستراتيجية، وتوفير الموارد الكافية والملائمة والفعالة، والتوفيق في عملية إتخاذ القرارات بين إهتمامات أصحاب المصالح نحو القيمة المضافة من جهة ومقارنة المخاطر مع العائد من خلال الاستغلال الامثل للموارد من جهة أخرى .

وعليه فإن الأهداف التي يسعى البنك للوصول إليها من خلال تبني اطار حاكمية تكنولوجيا المعلومات هي:

1. تلبية احتياجات أصحاب المصالح (Stakeholders needs) 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.
   - توفير بنية تحتية تكنولوجية متميزة وداعمه تمكن البنك من تحقيق أهدافه.
   - الإرتقاء بعمليات البنك المختلفة من خلال توظيف منظومة تكنولوجية كفؤة بمستوى اعتماد متميز.
   - 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، وذلك من خلال تعزيز أنظمة الضبط والرقابة الداخلية لدى البنك.
   - تحسين نظام الضبط والرقابة الداخلية.
   - 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.
2. تحقيق الشمولية في حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها ومن خلال توفير العناصر Components اللازمة.
3. تبني ممارسات وقواعد العمل والتنظيم بحسب أفضل المعايير الدولية كنقطة إنطلاق يتم الإرتكاز 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 الإدارة التنفيذية بخصوص المعلومات والتكنولوجيا المصاحبة لها.
5. تعزيز آليات الرقابة الذاتية والرقابة المستقلة وفحص الامتثال في مجالي حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها وبما يسهم في تحسين وتطوير الأداء بشكل مستمر.

كما وتعتبر أهداف الحاكمية والإدارة وباقي العناصر Components المرتبطه بنشاطات تتعلق بمواضيع الامن السيبراني وإدارة المخاطر وخصوصية وحماية البيانات والامتثال والمراقبه والتدقيق والتوافق الاستراتيجي عبارة عن (Focus Areas) ذات اهمية واولوية عليا.

الباب الثاني: إطار حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها المتبع لدى البنك (COBIT) والعناصر Components

أولاً : مبادىء حاكمية تكنولوجيا المعلومات:

تعمل المبادىء الرئيسة لحاكمية تكنولوجيا المعلومات على تمكين البنك من بناء إطار عمل فعال للحاكمية والإدارة يحسن من إستخدام المعلومات والإستثمارات في التقنيات بالشكل الأمثل، وفيما يلي المبادىء الرئيسية لحاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها ووفقاً لإطار COBIT:

1. تلبية إحتياجات أصحاب المصالح (Provide Stakeholder Value) :

أن الغرض الأساسي للبنك هو إيجاد قيمة مضافة لأصحاب المصالح وبالتالي تحقيق الفوائد بالتكلفة المثلى للموارد.

2. أسلوب شمولي (Holistic Approach):

يتم تطبيق نظام شامل للحاكمية المؤسسية وإدارة تقنية المعلومات.

3. نظام حاكمية حيوي (Dynamic Governance System) :

يتمتع نظام الحاكمية لدى البنك بأنه نظام حيوي وقابل للتغيير .

4. تلبية إحتياجات المؤسسة (Tailored to the enterprise needs) :

إن نظام الحاكمية لدى البنك مصمم لتلبية احتياجات المؤسسة من خلال تحديد الأولويات.

5. فصل الحاكمية عن الإدارة (Separating Governance From Management):

يعنى مجلس الادارة بتطبيق الحاكمية المؤسسية الرشيدة في البنك والفصل بين دور المجلس والادارة التنفيذية، وتتمثل مسؤولية الادارة التنفيذية بالمهام المطلوبة من المدير العام وكوادر الادارة التنفيذية الاخرى للقيام بالتخطيط، والبناء، والتشغيل، ومراقبة الأنشطة ومواءمتها مع التوجهات الموضوعة من قبل مجلس الادارة وذلك لتحقيق اهداف البنك الإستراتيجية.

6. تغطية المؤسسة من بدايتها لنهايتها (Covering the Enterprise End-to-end):

بحيث تعمل حاكمية التكنولوجيا على خلق تكامل بين حاكمية تكنولوجيا المعلومات والحاكمية المؤسسية بما يغطي جميع الوظائف والعمليات داخل البنك.

ثانياً : العناصر Components:

يتم تحقيق الشمولية في حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها من حيث الأخذ بالاعتبار ليس فقط التكنولوجيا بحد ذاتها وإنما توفير سبعة عناصر (7 Components) تكون مصاحبة ومكملة لخدمات تكنولوجيا المعلومات تتمثل بما يلي:

1. المبادئ والسياسات وأطر العمل(Principles, Policies and Frameworks)، والتي تعد وسائل لترجمة السلوكيات المرغوبة الى ارشادات عملية للإدارة اليومية.
2. العمليات (Processes)، والتي تمثل مجموعة منظمة من الممارسات والأنشطة لتحقيق أهداف معينة.
3. الهياكل التنظيمية (Organizational Structures).
4. الثقافة والأخلاقيات والسلوك (Culture, Ethics and Behavior)، من خلال منظومة القيم والأخلاق والسلوكيات الخاصة بالبنك.
5. المعلومات (Information)، وتشمل جميع المعلومات التي ينتجها ويستخدمها البنك، والتي هي ضرورية لتشغيل البنك وحوكمته بشكل جيد.
6. الخدمات والبرامج والبنية التحتية والتطبيقات (Services, Infrastructure and Applications)، المعنية في توفير المعالجة لتكنولوجيا المعلومات وتسهل تقديم الخدمات.
7. العنصر البشري والمهارات والكفاءات (People, Skills and Competencies)، والتي تعد ضرورية لنجاح إكتمال جميع الأنشطة وإتخاذ القرارات والإجراءات الصحيحة.

ولإنجاح الإطار العام لحاكمية تكنولوجيا المعلومات يلتزم البنك بتفعيل الدعامات السبع لتحقيق الشمولية الموجودة.

ويقوم البنك عند التطبيق والدخول في تفاصيل الدعامات السبعة والمرفقات والعمليات والأهداف الفرعية بتطويع (Tailoring) كل ذلك بما ينسجم ومعطيات البنك في سبيل خدمة أهداف ومتطلبات تعليمات حاكمية تكنولوجيا المعلومات و (COBIT) والعمل على إيجاد التغيير المطلوب لتوفير وتهيئة البيئة اللازمة للتطبيق من خلال اتباع أسلوب تحليل الفجوة (Gap Analysis) بين الوضع الحالي والمقارنة مع متطلبات وتعليمات المعيار لغايات الإلتزام بالتطبيق، ويلتزم البنك بإرسال تقرير الإنجاز المتعلق بالامتثال لتحقيق متطلبات تطبيق (COBIT) بشكل نصف سنوي للبنك المركزي الأردني، موضحاً فيه مستوى الإنجاز.

ثالثاً : عمليات حاكمية تكنولوجيا المعلومات:

يتكون الاطار العام لتطبيق حاكمية تكنولوجيا المعلومات (Cobit) من نطاقين عمليات رئيسيين هما:

1. نطاق عمليات مجلس الادارة: ويمكن تقسيمه لخمس عمليات وفي كل عملية يتم تعريف ممارسات التقييم Evaluate والتوجيه Direct والمراقبة Monitor والمعروفة باختصار (EDM5) والذي يقوم بالتأكد من وضع وصيانة اطار عمل حاكمية تكنولوجيا المعلومات، وتحقيق المنافع، وادارة المخاطر، والتأكد من الاستغلال الامثل للموارد، ومن التعامل بشفافية مع أصحاب المصالح.

2. نطاق عملية الادارة التنفيذية: ويحتوي على اربعة محاور متماشية مع مناطق مسؤوليات التخطيط Plan، والبناء Build، والتشغيل Operate، والمراقبة Monitor، والمعروفة اختصاراً بـ(PBRM)، وتوفر هذه المحاور تغطية شاملة لنطاق حاكمية تكنولوجيا المعلومات، وقد تم اختيار اسماء المحاور بما يتماشى مع دلالتها الرئيسة وهي:

- المواءمة والتخطيط والتنظيم (APO): تقوم باجراء صياغة سياسة تكنولوجيا المعلومات، واستراتيجية تكنولوجيا المعلومات، ووضع الهياكل التنظيمية لدى البنك، والإدارة المالية، وإدارة المحافظ الإستثمارية.
- البناء والاستحواذ والتنفيذ (BAI): وتعتبر اجراء تحليل الأعمال، وادارة المشاريع، وتقييم سيناريوهات الإستخدام، وتعريف المتطلبات وإدارتها، والبرمجة، وهندسة النظم، وإخراج النظم من الخدمة، وإدارة القدرات.
- الخدمة وصيانتها ودعمها(DSS): وهي اجراء إدارة الإتاحة (التوفر)، وإدارة المشاكل، وإدارة مكتب الخدمة والحوادث، وإدارة الأمن، وعمليات تقنية المعلومات، وادارة قاعدة البيانات.
- المراقبة والتقييم والتقدير(MEA): وتمثل اجراء مراجعة الامتثال (التوافق)، ومراقبة الكفاءة، وتدقيق ادوات الضبط.

ويلتزم البنك بالتنفيذ الأمثل للمحاور والعمليات المبينة وذلك لإنجاح التطبيق السليم لحاكمية تكنولوجيا المعلومات.

رابعاً : مستويات النضوج وقدرة الإجراءات:

يهدف استخدام مستويات النضوج لغايات تحسين الاجراءات وتقييم نضوج العمليات، وتحديد المستوى المستهدف والوقوف على الانحرافات، وهناك ستة مستويات يمكن تصنيف الاجراءات من خلالها، وهي:

- المستوى (0) الاجراء غير المكتمل (Incomplete process): وهو الانعدام التام لأية عمليات واضحة وبالتالي لم يدرك البنك ان هناك مشكلة يجب معالجتها.
- المستوى (1) الاجراءالاولي (Initial process): هناك أدلة بان البنك أدرك بان المشاكل قائمة ويجب معالجتها رغم ذلك ليس هناك اجراءات قياسية، بل ان هناك مقاربات مرتبطة بغرض معين يتم تطبيقها على اساس فردي او على اساس كل حالة بعينها، وبهذا فإن توجه البنك نحو الادارة بشكل عام غير منظم.
- المستوى (2) الاجراء منفذ (Performed process): تطور العمليات إلى المرحلة حيث يتم اتباع اجراءات مماثلة من قبل مختلف الافراد الذين يقومون بنفس المهمة، وليس هناك تدريب رسمي او نشر للاجراءات القياسية، وتترك المسؤولية للفرد، وهناك درجة عالية من الاعتماد على معرفة الافراد ولهذا السبب فان الاخطاء محتملة.
- المستوى (3) الاجراء محدد جداً (Well defined process): تم توثيق الاجراءات وتحديدها لتكون كإجراءات قياسية، ومن ثم نشرها في البنك عبر التدريب، وينص التوثيق على وجوب اتباع هذه الاجراءات، لكن من غير المرجح ان يتم كشف الانحرافات.
- المستوى (4) الاجراء القابل للقياس (Measured process) : تعمل الادارة على مراقبة وقياس مستوى الامتثال للسياسات وتتخذ اجراءات حيث تبدو العمليات لا تعمل بشكل فعال، وتكون الاجراءات خاضعة للتحسين المستمر وتقدم تجربة ناضجة للآخرين، كما تستخدم الأتمتة والادوات بطريقة محدودة او مجزأة.
- المستوى (5) الاجراء المستمر (Continuous process): في هذا المستوى تم تنقيح الاجراءات لتصل لمستوى الممارسة الرشيدة، وذلك بناء على نتائج التحسين المستمر وإعداد نماذج النضوج عبر المشاركة مع المؤسسات

الاخرى وهنا تستخدم تقنية تكنولوجيا المعلومات بطريقة متكاملة لاتمتة تدفق العمل، فتوفر الادوات لتحسين الجودة والفعالية وتمكن البنك من التكيف بسرعة.

ويتناسب مستوى نضوج (Capability Level) النشاطات المتعلقة بأهداف حاكمية تكنولوجيا المعلومات وباقي العناصر الستة Components المرتبطة بها بشكل طردي مع درجة الأهمية والأولوية بحسب نتائج الدراسة الكمية والنوعية، كما ويسعى البنك أن لا يقل مستوى النضوج للنشاطات ذات الأهمية والأولوية عن المستوى (3) (Fully Achieved) بحسب سلم النضوج الوارد في اطار العمل(Cobit)*، ويسعى البنك دائماً للوصول لمستويات أعلى من مستوى النضوج المطلوب.

* يسمح باعتبار ما لايزيد عن (26%) من أهداف الحاكمية والإدارة ضمن اهداف الادارة (بما لا يزيد عن 9 اهداف بحد أقصى من أصل 35 هدف) على انها ذات اهمية واولوية ادنى أو مهملة.

الباب الثالث: دور مجلس الإدارة في إدارة المعلومات والتكنولوجيا المصاحبة لها

تمثل الأدوار والأنشطة والعلاقات العناصر التي تحدد الجهات المعنية في الحاكمية وكيفية إشراكهم بعملية التطبيق، ومن أهم المبادىء التي تقوم عليها حاكمية تكنولوجيا المعلومات هي فصل المهام الخاصة بالمجلس عن الإدارة التنفيذية ويتم التمييز بين دور مجلس الإدارة وأنشطة الإدارة التنفيذية من خلال تحديد كيفية التواصل ما بين أصحاب المصالح والإدارة التنفيذية وفيما يلي المهام والمسؤوليات للجهات مدار البحث:

1. <u>مهام ومسؤوليات مجلس الإدارة:</u>

- المراقبة على أعمال الإدارة التنفيذية العليا بهدف التحقق من فعالية وكفاءة العمليات ومصداقية التقارير المالية ومدى الامتثال للقوانين والتشريعات والتعليمات النافذة وتلتزم الإدارة العليا بتطبيق المبادئ الأساسية لأنظمة الضبط والرقابة الداخلية ويكون مجلس الإدارة المسؤول المباشر لعمليات التقييم والتوجيه والرقابة وعن عملية "ضمان إدارة حصيفة لمخاطر تكنولوجيا المعلومات"، وعملية "إدارة المخاطر".
- 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 ومن وجود مراجعة فنية متخصصة (IT Audit)، من خلال كوادر مهنية مؤهلة ومعتمدة دوليا بهذا المجال، وحاصلين 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.
- يتولى المجلس ومن خلال لجنة حاكمية تكنولوجيا المعلومات والأمن السيبراني 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، والمتعلقة بإدارة مخاطر تكنولوجيا المعلومات، وإدارة أمن وحماية تكنولوجيا المعلومات، وإدارة الموارد البشرية والتي تلبي متطلبات عمليات حاكمية تكنولوجيا المعلومات ومنظومة السياسات اللازمة لإدارة موارد وعمليات حاكمية تكنولوجيا المعلومات، والعمل بهذه السياسات بشكل متكامل مع سياسات البنك الأخرى الناظمة لأعماله ومواءمة الأهداف وآليات العمل ويتم الالتزام بتحديد الجهة المالكة ونطاق التطبيق ودورية المراجعة والتحديث وصلاحيات الاطلاع والتوزيع والأهداف والمسؤوليات وإجراءات العمل المتعلقة بها والعقوبات في حال عدم الامتثال وآليات فحص الامتثال، ويراعى لدى إنشاء السياسات مساهمة كافة الشركاء الداخليين والخارجيين واعتماد أفضل الممارسات الدولية وتحديثاتها.
- اعتماد الهياكل التنظيمية (الهرمية واللجان) الخاصة بإدارة موارد وعمليات ومشاريع تكنولوجيا المعلومات، وإدارة مخاطر تكنولوجيا المعلومات، وإدارة أمن المعلومات، وإدارة الموارد البشرية والتي تلبي متطلبات عمليات حاكمية تكنولوجيا المعلومات وتحقيق أهداف البنك بكفاءة وفعالية ومراعاة ضمان فصل المهام والرقابة الثنائية كحد أدنى وكفاية وتحديث الوصف الوظيفي لدى اعتماد وتعديل الهياكل التنظيمية للبنك.

- تطوير البنية التحتية ونظم المعلومات اللازمة لتوفير المعلومات والتقارير لمستخدميها كمرتكز لعمليات اتخاذ القرار في البنك، حيث يجب أن تتوفر متطلبات جودة المعلومات (Information Quality Criteria) والمتمثلة بالمصداقية (Integrity Completeness, Accuracy and Validity or Currency)، ومتطلبات السرية بحسب سياسة تصنيف البيانات ومتطلبات التوافرية والامتثال بتلك المعلومات والتقارير، بالإضافة للمتطلبات الأخرى الواردة في (COBIT) وتمكين المعلومات (Information Enabling).
- يتولى المجلس ومن خلال لجنة حاكمية تكنولوجيا المعلومات والأمن السيبراني اعتماد منظومة المعلومات والتقارير واعتبار تلك المنظومة حدا أدنى، مع مراعاة تحديد مالكين لتلك المعلومات والتقارير تحدد من خلالهم وتفوض صلاحيات الاطلاع والاستخدام بحسب الحاجة للعمل والشركاء المعنيين، ويتم مراجعتها وتطويرها بشكل مستمر لمواكبة تطور أهداف وعمليات البنك وبما يتفق وأفضل الممارسات الدولية المقبولة بهذا الخصوص.
- يتولى المجلس ومن خلال لجنة حاكمية تكنولوجيا المعلومات والأمن السيبراني اعتماد منظومة الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات الداعمة والمساعدة لتحقيق عمليات حاكمية تكنولوجيا المعلومات وبالتالي أهداف المعلومات والتكنولوجيا المصاحبة لها، وبالتالي الأهداف المؤسسية، واعتبار تلك المنظومة حداً أدنى، ويتم توفيرها وتطويرها بشكل مستمر لمواكبة تطور أهداف وعمليات البنك وبما يتفق وأفضل الممارسات الدولية المقبولة بهذا الخصوص.
- يتولى المجلس ومن خلال لجنة حاكمية تكنولوجيا المعلومات والأمن السيبراني ولجنة الترشيحات والمكافآت اعتماد مصفوفة المؤهلات (HR Competencies) وسياسات إدارة الموارد البشرية اللازمة لتحقيق متطلبات عمليات حاكمية تكنولوجيا المعلومات وعلى أساس الجدارة، ويلتزم المجلس والإدارة التنفيذية العليا بتوظيف الآليات المختلفة لتشجيع تطبيق السلوكيات المرغوبة وتجنب السلوكيات غير المرغوبة من خلال اتباع أساليب الحوافز والعقوبات.
- يتولى المجلس ومن خلال لجنة حاكمية تكنولوجيا المعلومات والأمن السيبراني ولجنة التدقيق 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.

2. <u>لجنة حاكمية تكنولوجيا المعلومات والأمن السيبراني:</u>

لغايات تلبية المهام المطلوبة من مجلس الإدارة آنفة الذكر، تم تشكيل لجنة حاكمية تكنولوجيا المعلومات والأمن السيبراني بقرار من مجلس الإدارة مكونه من أربعة أعضاء من مجلس الإدارة من ذوي الخبرة والمعرفة الاستراتيجية في تكنولوجيا المعلومات، وتم تعيين رئيس للجنة من بين الأعضاء الأربعة، وتجتمع اللجنة بشكل ربع سنوي على الأقل وتحتفظ بمحاضر اجتماعات موثقة، ويتم رفع تقارير دورية للمجلس، هذا وتتلخص مهام اللجنة فيما يلي:

- التأكد من وجود المواءمة والتوافق بين الخطة الإستراتيجية العامة للبنك التجاري الأردني وخطة دائرة تكنولوجيا المعلومات الإستراتيجية بما يضمن تحقيق أهداف البنك الإستراتيجية.
- التأكد من تطبيق خدمات تقنية المعلومات بما يخدم الحد من المخاطر.

- متابعة مؤشرات الأداء ومراقبة تطبيق وتحقيق الإستراتيجية العامة، سير المشاريع، استغلال الموارد والاستفادة منها، ومؤشرات جودة تقديم الخدمات، وبطاقات الأهداف المتوازنة التي تعكس تحقيق الأهداف الإستراتيجية.
- التأكد من وجود الاستثمار الأمثل للموارد المتاحة، سواء كانت أنظمة حساسة، معلومات، بنية تكنولوجيا المعلومات التحتية، والموظفين.
- اعتماد الأهداف الاستراتيجية لتكنولوجيا المعلومات وحوكمة الأمن السيبراني والهياكل التنظيمية المناسبة بما في ذلك اللجان التوجيهية على مستوى الإدارة التنفيذية العليا وعلى وجه الخصوص (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 الإستثمار (Return On Investment) (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 2019) (Control Objectives for Information and related Technology)، يتوافق ويلبي تحقيق أهداف ومتطلبات التعليمات من خلال تحقيق الأهداف المؤسسية بشكل مستدام، وتحقيق مصفوفة أهداف الموائمة ويغطي أهداف الحاكمية والإدارة.
- اعتماد مصفوفة الأهداف المؤسسية، وأهداف الموائمة واعتبار معطياتها حداً أدنى، وتوصيف الأهداف الفرعية اللازمة لتحقيقها.
- اعتماد مصفوفة للمسؤوليات (RACI Chart) تجاه العمليات الرئيسية لأهداف الحاكمية والإدارة 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 2019 بهذا الخصوص.
- 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.
- 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.
- الإطلاع على تقارير التدقيق لتكنولوجيا المعلومات واتخاذ ما يلزم من اجراءات لمعالجة الإنحرافات.
- التوصية للمجلس باتخاذ الإجراءات اللازمة لتصحيح أية إنحرافات.
- الاطلاع على سياسة وبرنامج الأمن السيبراني واعتمادها من مجلس الإدارة والإشراف والتأكد من الإمتثال لسياسة وبرنامج الأمن السيبراني وتحديد الأدوار والمسؤوليات المتعلقة بالأمن السيبراني.
- التأكد من إنشاء نظام وآلية لإدارة الخدمات المقدمة من الطرف الثالث بغرض دعم عملية تقديم خدمات البنك.
- تضمن لجنة حاكمية تكنولوجيا المعلومات والأمن السيبراني استقلالية وحدة أمن المعلومات وبحيث تتبع إدارياً لدائرة المخاطر وتقوم اللجنة التوجيهية بالإطلاع على محاضر الإجتماع التي تتضمن التقارير الدورية التي تقوم بإعدادها وحدة أمن المعلومات ورفعها الى اللجنة التوجيهية لحاكمية تكنولوجيا المعلومات والأمن السيبراني فيما يخص الأمن السيبراني في البنك، والانحرافات المتعلقة بتطبيق سياسة الأمن السيبراني وإجراءاتها، ونتائج تقييم المخاطر السيبرانية، ونتائج تقييم مدى كفاية وكفاءة برنامج وسياسة الأمن السيبراني، والتوصيات والإجراءات والمتطلبات الواجبة التنفيذ، ملخص يستعرض أهم أحداث تهديدات واختراقات الأمن السيبراني خلال فترة التقرير.
- اعتماد أهمية وترتيب أولوية أهداف الحاكمية والإدارة ومدى ارتباطها في الاهداف المؤسسية وأهداف الموائمة، بالإضافة لارتباطها بباقي العناصر الستة Components، وذلك بناء على دراسة نوعية و/أو كمية تعد لهذا الغرض بشكل سنوي على الاقل تأخذ بعين الاعتبار ال (Design Factors) الواردة في (COBIT 2019 – Design Guide).
- اعتماد تقرير التدقيق السنوي بتقييم (مخاطر–ضوابط) المعلومات والتكنولوجيا المصاحبة لها للبنك.
- مراقبة واعتماد مستوى المخاطر السيبرانية بشكل مستمر ومدى قدرة البنك على تحمل المخاطر السيبرانية، وبحيث تكون المخاطر السيبرانية الإجمالية ضمن النطاق المقبول.
- التأكد من توفر برنامج التوعية بالأمن السيبراني بالبنك، وإدراك الآثار القانونية والتنظيمية للمخاطر السيبرانية.
- تخصيص الميزانية والموارد الكافية لتلبية متطلبات الأمن السيبراني.
- الدعم والمشاركة في تقييمات مرونة المخاطر السيبرانية وأي مبادرات متعلقة بالأمن السيبراني.

3. <u>لجنة التدقيق:</u>

- 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 مع متطلبات الجهات الرقابية.
- التأكيد للمجلس من قيام المدقق الداخلي والمدقق الخارجي للبنك لدى تنفيذ عمليات التدقيق المتخصص للمعلومات والتكنولوجيا المصاحبة لها الإلتزام 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 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.

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 المطلوبة، علماً بأن درجات التقييم للمخاطر تنقسم تنازلياً الى خمسة مستويات (عبارة عن سلم التقييم الكلي للمخاطر Composite Risk Rating) : قوي (Strong Performance, Rate 1)، ومرضي (Satisfactory Performance, Rate 2)، وعادل (fair Performance, Rate 3)، وحدي (Marginal Performance, Rate 4)، وغير مرضي (Unsatisfactory Performance, Rate 5).

وعلى أن يكون تكرار التدقيق لكافة المحاور أو جزء منها كحد أدنى مرة واحدة سنوياً على الأقل في حال تم تقييم المخاطر بدرجة (5 أو 4) بحسب سلم تقييم المخاطر، 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 أو 1)، مع مراعاة التغير المستمر في مستوى المخاطر والأخذ بعين الإعتبار التغيرات الجوهرية التي تطرأ على بيئة المعلومات والتكنولوجيا المصاحبة لها خلال فترات التدقيق المذكورة، على أن يتم تزويد البنك المركزي بتقارير

التدقيق والتي تشمل عمليات التقييم للمحاور المذكورة وآليات البنك المتبعة من حيث التخطيط الاستراتيجي ورسم السياسات والمبادئ وإجراءات العمل المكتوبة والمعتمدة، وآليات توظيف الموارد المختلفة بما فيها موارد تكنولوجيا المعلومات والعنصر البشري، وآليات وأدوات المراقبة والتحسين والتطوير، والعمل على توثيق نتائج التدقيق وتقييمها اعتمادا على أهمية الاختلالات ونقاط الضعف(الملاحظات) بالإضافة للضوابط المفعلة وتقييم مستوى المخاطر المتبقية والمتعلقة بكل منها باستخدام معيار منهجي لتحليل وقياس المخاطر، متضمنا الإجراءات التصحيحية المتفق عليها والمنوي اتباعها من قبل إدارة البنك بتواريخ محددة للتصحيح، مع الإشارة ضمن جدول خاص إلى رتبة صاحب المسؤولية في البنك المعني بالملاحظة، وتزويد البنك المركزي الأردني بتقرير سنوي للتدقيق الداخلي وآخر للتدقيق الخارجي على التوالي يتضمن رد الإدارة التنفيذية وإطلاع وتوصيات المجلس بخصوصه، ووفق نموذج تقرير تدقيق (مخاطر-ضوابط) المعلومات والتكنولوجيا المصاحبة لها، وذلك خلال الربع الأول من كل عام.

3. إجراءات منتظمة لمتابعة نتائج التدقيق للتأكد من معالجة الملاحظات والاختلالات الواردة في تقارير المدقق بالمواعيد المحددة، والعمل على رفع مستوى الأهمية والمخاطر تصعيدا تدريجيا في حال عدم الاستجابة ووضع المجلس بصورة ذلك كلما تطلب الأمر.
4. 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 لدوائر التدقيق.
5. اعتماد منظومة الأخلاق والممارسات المهنية الواردة في المعيار الدولي (Information Technology Assurance Framework) (ITAF) الصادر عن جمعية التدقيق والرقابة على نظم المعلومات (ISACA) وتحديثاته الذي يجب على المدقق الداخلي والمدقق الخارجي الامتثال لها.

يمكن أن يقوم البنك بإسناد(Outsource) دور المدقق الداخلي للمعلومات والتكنولوجيا المصاحبة لها (Internal IT Audit) لجهة خارجية متخصصة مستقلة عن المدقق الخارجي المعتمد، شريطة تلبية كافة متطلبات تعليمات حاكمية تكنولوجيا المعلومات وأية تعليمات أخرى ذات صلة ويحتفظ مجلس الإدارة ولجنة التدقيق المنبثقة عنه بدورهما فيما يتعلق بفحص الامتثال والتأكد من تلبية المتطلبات كحد أدنى.

الباب الرابع: دور الإدارة التنفيذية في إدارة المعلومات والتكنولوجيا المصاحبة لها

1. مسؤوليات ومهام الإدارة التنفيذية العليا:

- توظيف العنصر البشري المؤهل والمدرب من الأشخاص ذوي الخبرة في مجالات إدارة موارد تكنولوجيا المعلومات وإدارة المخاطر وإدارة أمن المعلومات وإدارة تدقيق تكنولوجيا المعلومات اعتمادا على معايير المعرفة الأكاديمية والمهنية والخبرة العملية باعتراف جمعيات دولية مؤهلة بموجب معايير الاعتماد الدولي للمؤسسات المانحة للشهادات المهنية (ISO/IEC 17024) و/أو أية معايير أخرى موازية كل بحسب اختصاصه وبما يتفق مع سياسات البنك وبرفد الموظفين ببرامج التدريب والتعليم المستمر للحفاظ على مستوى من المعارف والمهارات يلبي ويحقق عمليات حاكمية تكنولوجيا المعلومات.
- اعتماد منظومة الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات الداعمة والمساعدة لتحقيق عمليات حاكمية تكنولوجيا المعلومات وبالتالي أهداف المعلومات والتكنولوجيا المصاحبة لها، وبالتالي الأهداف المؤسسية، وتوفيرها وتطويرها بشكل مستمر لمواكبة تطور أهداف وعمليات البنك وبما يتفق وأفضل الممارسات الدولية المقبولة.
- تضمين آليات التقييم السنوي (Performance Evaluation) للكوادر بمعايير قياس موضوعية تأخذ بعين الاعتبار المساهمة من خلال المركز الوظيفي بتحقيق أهداف البنك.
- تطوير البنية التحتية ونظم المعلومات اللازمة لتوفير المعلومات والتقارير لمستخدميها كمرتكز لعمليات اتخاذ القرار في البنك، وعليه يجب أن تتوفر متطلبات جودة المعلومات (Information Quality Criteria) والمتمثلة بالمصداقية (Integrity Completeness, Accuracy and Validity or Currency)، ومتطلبات السرية بحسب سياسة تصنيف البيانات ومتطلبات التوافرية والامتثال بتلك المعلومات والتقارير، بالإضافة للمتطلبات الأخرى الواردة في (COBIT – Enabling Information) .
- توظيف الآليات المختلفة لتشجيع تطبيق السلوكيات المرغوبة وتجنب السلوكيات غير المرغوبة من خلال اتباع أساليب الحوافز والعقوبات.

2. اللجنة التوجيهية لتكنولوجيا المعلومات والامن السيبراني:

تم تشكيل لجنة توجيهية لتكنولوجيا المعلومات والأمن السيبراني تضمن عملية التوافق الاستراتيجي لتكنولوجيا المعلومات لتحقيق الأهداف الاستراتيجية للبنك بشكل مستدام، وتتكون من رئيس اللجنة السيد المدير العام وعضوية مدراء الإدارة التنفيذية العليا بما في ذلك مدير تكنولوجيا المعلومات ومدير إدارة المخاطر ومسؤول أمن المعلومات، كما تم انتخاب أحد أعضاء المجلس ليكون عضواً مراقباً في هذه اللجنة بالإضافة للمدقق العام/بصفة مراقب، ويمكنها دعوة الغير لدى الحاجة لحضور اجتماعاتها، وتوثق اللجنة اجتماعاتها بمحاضر أصولية، على أن تكون دورية الاجتماعات مرة كل ثلاثة أشهر على الأقل، هذا وتتلخص مهام اللجنة فيما يلي:

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 أهداف التوافق المصاحبة لها واعتمادها ومراجعتها بشكل مستمر وبما يضمن تحقيق الأهداف الاستراتيجية للبنك وأهداف تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها، ومراعاة تعريف مجموعة معايير للقياس ومراجعتها وتكليف المعنيين من الإدارة التنفيذية بمراقبتها بشكل مستمر وإطلاع اللجنة على ذلك.
3. التوصية بتخصيص الموارد المالية وغير المالية اللازمة لتحقيق الأهداف وعمليات حاكمية تكنولوجيا المعلومات، والاستعانة بالعنصر البشري الكفوء والمناسب من خلال هياكل تنظيمية تشمل كافة العمليات اللازمة لدعم الأهداف تراعي فصل المهام وعدم تضارب المصالح، وتطويع البنية التحتية التكنولوجية والخدمات الأخرى المتعلقة بها خدمة للأهداف، وتولي عمليات الإشراف على سير تنفيذ مشاريع وعمليات حاكمية تكنولوجيا المعلومات.
4. ترتيب مشاريع وبرامج تكنولوجيا المعلومات بحسب الأولوية.
5. مراقبة مستوى الخدمات الفنية والتكنولوجية والعمل على رفع كفاءتها وتحسينها بشكل مستمر.
6. رفع التوصيات اللازمة للجنة حاكمية تكنولوجيا المعلومات والأمن السيبراني بخصوص الأمور التالية:
- تخصيص الموارد اللازمة والآليات الكفيلة بتحقيق مهام لجنة حاكمية تكنولوجيا المعلومات والأمن السيبراني.
- أية إنحرافات قد تؤثر سلبا على تحقيق الأهداف الاستراتيجية.
- أية مخاطر غير مقبولة متعلقة بتكنولوجيا وأمن وحماية المعلومات.
- تقارير الأداء والامتثال بمتطلبات الإطار العام لإدارة وضبط ومراقبة موارد ومشاريع تكنولوجيا المعلومات.
7. تزويد لجنة حاكمية تكنولوجيا المعلومات والأمن السيبراني بمحاضر اجتماعاتها أولا بأول والحصول على ما يفيد الاطلاع عليها.

ويكون مدير دائرة هندسة العمليات مقرراً للجنة.

المراجع :

1. تعليمات الحاكمية المؤسسية رقم (2023/2) تاريخ 2023/02/14 الصادرة عن البنك المركزي الأردني.
2. تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم (2016/65) تاريخ 2016/10/25 الصادرة عن البنك المركزي الأردني والتعميم اللاحق للتعليمات رقم (10/6/984) تاريخ 2019/01/21 الصادرة عن البنك المركزي الأردني.
3. COBIT 2019 Framework – Introduction and Methodology الصادرة عن جمعية التدقيق والرقابة على نظم المعلومات (ISACA) في الولايات المتحدة الامريكية.