بنك القاهرة عمّان
CairoAmmanBank

قرار مجلس الإدارة

المتخذ بتاريخ 2023/12/19

الموضوع: دليل حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها

قرر مجلس الإدارة في جلسته المنعقدة بتاريخ 2023/12/19 الموافقة على دليل حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها المرفق طيه نسخة عنه.

يزيد المفتي

رئيس مجلس الإدارة

SCANWAVE

ISACA®

دليل حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها

بنك القاهرة عمّان
CairoAmmanBank

بنك القاهرة عمّان
CairoAmmanBank

تاريخ المراجعات

الحدث	التاريخ	جهة اعتماد	الاسم	رقم النسخة
المؤلف				
المدقق				

تم تطوير هذا الدليل بناء على تعليمات البنك المركزي الأردني رقم **65/2016** و تعميم 10-6-984 وإطار كويت 2019 الصادر عن جمعية التدقيق والرقابة على نظم المعلومات **ISACA**

المحتويات

1. المقدمة.....4
2. لمحة عامة عن بنك القاهره عمان.....5
3. النطاق.....6
4. الأهداف.....7
5. السياسات العامة.....8
6. وضع الأهداف وتتابعها.....15
الملحق أ : منظومة السياسات(حد أدنى).....16
الملحق ب: الحد الأدنى من التقارير والمعلومات.....19
الملحق ج: الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات.....20
التعريفات.....21

1. المقدمة

يدرك بنك القاهره عمان ممثلا بمجلس الإدارة وإدارته التنفيذيه أهمية دور تكنولوجيا المعلومات كبقية الوحدات المصرفية العاملة في البنك. حيث عمل البنك ممثلا بمجلس الإدارة وإدارته التنفيذية وبكافة وحدات الأعمال سواء كانت وحدات مصرفية أو تكنولوجيا المعلومات على التعاون والعمل سوية لضم تكنولوجيا المعلومات تحت مظلة الحاكمية وأسلوبها الإداري.

واستجابة لتعليمات البنك المركزي الأردني رقم 65/2016 وتعميم 10-6-984، والتي تنسجم وتكمل للتعليمات رقم 2014/85 تاريخ 30/09/ 2014و رقم 2015/16 تاريخ 2015/5/21 ، قام البنك بالمبادرة لاعتماد إطار كوبت 2019 لحاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها إمتثالا للتعليمات الصادرة بهذا الخصوص.

كوبت 2019 يوفر إطار شامل يساعد البنك في تحقيق أهدافه المتعلقة بحاكمية وإدارة تكنولوجيا المعلومات على مستوى البنك بشكل كامل. حيث أن هذا الإطار يساعد البنك بالوصول إلى أعلى درجات الفائدة من تكنولوجيا المعلومات من خلال الحفاظ على التوازن بين أعلى فائدة من تكنولوجيا المعلومات وبأقل المخاطر والموارد. يمكن الإطار كوبت تكنولوجيا المعلومات من التطبيق الكلي للحاكمية والإدارة لكافة وحدات الأعمال في البنك، أي بمعنى آخر تغطية لكافة الأعمال ووظائف تكنولوجيا المعلومات ومسؤولياتها في البنك.

2. لمحة عامة عن بنك القاهرة عمان

منذ تأسيسه كشركة مساهمة عامة اردنيه في الحادي عشر من حزيران عام 1960، حرص بنك القاهرة عمان على توظيف قاعدته الرأسمالية القوية وخبرته العريقة الممتدة على مدار ستون عاما، للقيام بدور رائد و متميز في خدمة الاقتصاد الوطني عبر تقديمه لمجموعة شاملة ومتميزة من الخدمات والحلول المصرفية الناجحة التي تلبي كافة الاحتياجات المتنوعة لعملائه. كما أضافت خدماته الرائدة بعداً جديداً للعديد من المشاريع في المجتمع، وذلك من خلال تمويل المشاريع التنموية بالإضافة إلى توفير الاحتياجات التمويلية للمشاريع الصغيرة والمتوسطة وحتى المتناهية الصغر التي ترفد الاقتصاد الأردني، إضافة إلى تلبية احتياجات عملائه الآنية بتوفير القروض الشخصية عبر تحويل الراتب و توفير خدمات الاستثمار وبطاقات الائتمان والتحويلات البنكية من خلال شبكة متميزة ومتكاملة من الفروع المصرفية في الأردن وفلسطين والبحرين، يقدم بنك القاهرة عمان لعملائه مجموعة متنوعة من الخدمات المصرفية المبتكرة التي تناسب كافة شرائح العملاء وتلبي كافة احتياجاتهم المصرفية والمالية والاستثمارية. كما يقدم البنك باقة من الخدمات المصرفية الإلكترونية من خلال موقعه الإلكتروني www.cab.jo التي توفر للعملاء إمكانية إجراء المعاملات المصرفية أينما تواجدوا. وتعكس هذه الخدمات المتميزة الهوية المؤسسية الجديدة للبنك، التي تجسّد روح الحداثة وقيم الانفتاح والتواصل لخدمة جميع المتعاملين معه وتحقيق الفوائد القصوى بعيداً عن الحدود التقليدية، ومن هذا المنطلق، عمل البنك جاهداً لتغطية كافة مناطق المملكة عن طريق تواجده في مراكز للبريد الأردني.

انطلاقاً من حرص البنك على تسهيل خدمة العملاء يضع بنك القاهرة عمان بين يدي عملائه شبكة صراف آلي واسعة الانتشار في مختلف مناطق الأردن و فلسطين ، ويفخر بكونه البنك الأول في العالم الذي يستخدم تقنية بصمة العين كوسيلة لدخول العميل إلى حسابه المصرفي والاستغناء عن بطاقات الصراف الآلي ورقم المرور (الرقم السري)، بحيث يقوم النظام بالتعرّف على هوية العميل وتمكينه من الدخول إلى حسابه سواء من خلال حاجز الخدمة لدى الفروع أو من خلال الصراف الآلي وإجراء معاملاته المصرفية، بهدف التسهيل على العملاء وتوفير الحماية والسلامة الكافية لهم لإيمانه بالريادة في استخدام التكنولوجيا الحديثة في القطاع المصرفي.

بكفاءة مصرفية و استثمارية ومالية، وبخبرات متميزة ، نسير قدماً لرفد الاقتصاد الوطني وتقديم الخدمات المصرفية الرائدة التي ترتقي بمستوى الفرد في الأردن.

3. النطاق

ينطبق هذا الدليل على كافة عمليات بنك القاهره عمان التي تعتمد على تكنولوجيا المعلومات بكافة دوائر وفروع البنك. يجب على كافة أصحاب المصالح مراعاة الإمتثال لهذه التعليمات وكل حسب مسماه و موقعة الوظيفي.

ينطبق هذا الدليل ايضا عند توقيع اتفاقيات الاسناد مع الغير لتوفير الموارد البشرية والخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات بهدف تسيير عمليات البنك والخدمات والبرامج والبنية التحتية المقدمة قبل وأثناء فترة التعاقد، وبما لا يعفي المجلس والإدارة التنفيذية العليا من المسؤولية النهائية لتحقيق متطلبات التعليمات.

القائمة أدناه تمثل الأطراف الرئيسية ومسؤلياتها بهذا الخصوص:

- رئيس وأعضاء المجلس: تولي مسؤوليات التوجيه العام للمشروع / البرنامج والموافقة على المهام والمسؤوليات ضمن المشروع، والدعم وتقديم التمويل اللازم .
- الخبراء الخارجيين المستعان بهم.
- الرئيس التنفيذي و رؤساء المجموعات ومدراء العمليات التنفيذين والفروع: تولي مسؤوليات تسمية الأشخاص المناسبين من ذوي الخبرة بعمليات البنك لتمثيلهم في المشروع وتوصيف مهامهم ومسؤولياتهم .
- مدير ولجان تكنولوجيا المعلومات التوجيهية ومدراء المشاريع: تولي مسؤوليات إدارة المشروع البرنامج وتوجيهه والإشراف عليه بشكل مباشر والتوصية بتوفير الموارد اللازمة لإتمامه، والتأكد من الفهم الصحيح من قبل كافة الأطراف بمتطلبات وأهداف التعليمات .
- التدقيق الداخلي: تولي مسؤولياته المناطة به بموجب التعليمات بشكل مباشر،و المشاركة 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 بالإطار COBIT المستعان بهم من داخل البنك ومن خارجه: تولي دور المرشد لنشر المعرفة بالإطار وتسهيل عملية التطبيق.
- وفقا لتعليمات البنك المركزي الأردني، يتحمل مجلس الإدارة المسؤولية المباشرة لعمليات الحوكمة الخمس (التقييم والتوجيه والمراقبة).
- يتولى مجلس الإدارة وإدارة المخاطر المسؤولية المباشرة عن عملية ضمان تقليل المخاطر (EDM03) وعملية إدارة المخاطر (APO12) .

4. الأهداف

وضع بنك القاهره عمان الأهداف التالية لإطار حاكمية وإدارة المعلومات والتكنولوجيا المصاحبه لها:

4.1. تلبية احتياجات أصحاب المصالح وتحقيق أهداف البنك من خلال تحقيق أهداف المعلومات والتكنولوجيا المصاحبة لها، وبما يضمن:

- توفير معلومات ذات جودة عالية كمرتكز يدعم آليات صنع القرارفي البنك.
- إدارة حصيفة لموارد ومشاريع تكنولوجيا المعلومات، تعظم الاستفادة من تلك الموارد وتقلل الهدر منها.
- توفير البنية التحتية التكنولوجية التي تمكن البنك من تحقيق أهدافه.
- الإرتقاء 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 رضا مستخدمي تكنولوجيا المعلومات من خلال تلبية احتياجات عملهم بكفاءة وفعالية.
- إدارة خدمات الأطراف الخارجية الموكل إليها تنفيذ عمليات ومهامو خدمات و منتجات.

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

4.3. تحقيق الشمولية في حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها من حيث الأخذ بالاعتبار ليس فقط التكنولوجيا بحد ذاتها وانما توفير عناصر تمكين (دعامات) تكون مصاحبة ومكملة لخدمات تكنولوجيا المعلومات تتمثل بـ: ١. المبادئ والسياسات وأطر العمل، ٢. عمليات حاكمية تكنولوجيا المعلومات، ٣. الهياكل التنظيمية، ٤. المعلومات والتقارير، ٥. الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات، ٦.المعارف والمهارات والخبرات، ٧. منظومة القيم والأخلاق والسلوكيات.

4.4. تبني ممارسات وقواعد العمل والتنظيم بحسب أفضل المعايير الدولية كنقطة إنطلاق يتم الإرتكاز والبناء عليها في مجالي حاكمية وإدارة عمليات ومشاريع وموارد تكنولوجيا المعلومات.

4.5. تعزيز آليات الرقابة الذاتية والرقابة المستقلة وفحص الامتثال في مجالي حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها وبما يسهم في تحسين وتطوير الأداء بشكل مستمر.

5. السياسات العامة

5.1. يستند هذا الدليل إلى تعليمات البنك المركزي الأردني رقم: 65/2016 وتعميم 10-6-984 ، والتي جاءت إعتمادا على إطار كوبت وينبغي مراجعة وتحديث هذا الدليل بشكل منتظم وبما يتواءم مع التحديثات التي تطرأ على هذا الاطار.

5.2. يتم اعتماد الدليل من مجلس الادارة. ويقوم البنك، من خلال لجنة حاكمية تكنولوجيا المعلومات المنبثقة عن مجلس الإدارة، بمراجعة هذا الدليل وتحديثه عند الضرورة. ويعبر هذا الدليل عن نظرة البنك الخاصة لحاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها من حيث مفهومها وأهميتها ومبادئها الأساسية.

5.3. يقوم البنك، بنشر هذا الدليل على الموقع الإلكتروني للبنك ومن خلال أي طريقة مناسبة. و يفصح البنك في تقريره السنوي عن وجود دليل خاص لحاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها أو متضمن لدليل الحاكمية المؤسسية لديه،ويفصح أيضاً عن المعلومات التي تهم أصحاب المصالح بما فيها الدليل،وعن مدى التزامه بتطبيق ما جاء فيه.

5.4. يعتمد بنك القاهره عمان برنامج أمن سيبراني شامل ومجموعه من السياسات والاجراءات الخاصة بالامن السيبراني بما يتناسب مع تعليمات البنك المركزي الاردني ويعتبر هذا البرنامج جزءا من اطار عمل البنك على حاكمية وادارة التكنولوجيا والمعلومات المصاحبة لها.

5.5. تعتبر الأهداف و عمليات حاكمية تكنولوجيا المعلومات بحسب المرفقين أرقام (٢) و(٣) على التوالي ومعطياتها حدا أدنى يتوجب على إدارة البنك العليا الامتثال لها وتحقيقها بشكل مستمر، وتعتبر اللجنة التوجيهية لتكنولوجيا المعلومات المسؤول الأول عن ضمان الامتثال بتحقيق متطلباتها، ولجنة حاكمية تكنولوجيا المعلوماتو المجلس 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 و تغطي متطلبات كافة عمليات حاكمية تكنولوجيا المعلومات الواردة في المرفق رقم (٣).

5.6. **اللجان**

- **لجنة حاكمية تكنولوجيا المعلومات:**

تماشيا مع تعليمات البنك المركزي الأردني، قام مجلس الاداره بتشكيل لجنة من أعضاء مجلس الإدارة تعنى بحاكمية تكنولوجيا المعلومات ، وتتكون هذه اللجنة من ثلاثة أعضاء على ا لأقل، وتضم في عضويتها أهل الخبرة والمعرفة 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 إداريي البنك لحضور اجتماعاتها للاستعانة برأيهم بمافيهم المعنيين في التدقيق الداخلي و أعضاء الإدارة التنفيذية العليا مثل المدير التنفيذي لادارة تكنولوجيا المعلومات وإدارة المشاريع 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،

تجتمع هذه اللجنة بشكل ربع سنوي على الأقل، ويتم الاحتفاظ بسجلات ومحاضر الاجتماع وتوثق حسب الأصول. وتتولى المهام التالية:

- 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) احتساب معدل العائد على (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)، يتوافق ويلبي تحقيق أهداف ومتطلبات تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها من خلال تحقيق الأهداف المؤسسية الواردة المبينة في التعليمات المذكورة بشكل مستدام،وتحقيق مصفوفة أهداف المعلومات والتكنولوجيا المصاحبة لها، ويغطي عمليات حاكمية تكنولوجيا المعلومات.
- اعتماد مصفوفة الأهداف المؤسسية الواردة في المرفق رقم (1) من تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها والتحديث الوارد عليها في تعميم البنك المركزي 10-6-984، وأهداف المعلومات والتكنولوجيا المصاحبة لها الواردة في المرفق رقم (2) والتحديث الوارد عليها في تعميم البنك المركزي 10-6 -984 واعتبار معطياتها حدا أدنى، وتوصيف الأهداف الفرعية اللازمة لتحقيقها.
- اعتماد مصفوفة للمسؤوليات (RACI Chart)تجاه العمليات الرئيسية لحاكمية تكنولوجيا المعلومات في المرفق رقم (3) والتحديث الوارد عليها في تعميم البنك المركزي 10-6-984 والعمليات الفرعية المنبثقة علها عن 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 في المرفق المذكور مسترشدين بمعيار COBIT 2019بهذا الخصوص.

- اعتماد أهمية ترتيب أولوية أهداف المؤسسة (Enterprise Goals)

  ومدى ارتباطها بأهداف التوافق (Alignment Goals)

  واهداف الحاكمية و الإدارة (Governance and Management Objectives)

  بالإضافة لارتباطها بباقي عناصر التمكين (Enablers/Components)

وذلك بناء على دراسة نوعية و/أو كمية تعد لهذا الغرض بشكل سنوي على الأقل تأخذ بعين الاعتبار العوامل المؤثرة في تشكيل إطار حاكمية تكنولوجيا المعلومات (COBIT 2019-Design factors)بما يتناسب مع خصوصية واستراتيجيات البنك بشكل عام و استراتيجية إدارة تقنية المعلومات المصوغة من قبل إدارة تقنية المعلومات و دائرة الاستراتيجية بشكل خاص ، على أن يتم تضمين مواضيع الأمن السيبراني، وإدارة المخاطر وخصوصية و حماية البيانات والامتثال والمراقبة والتدقيق والتوافق الاستراتيجي على أنها Focus Area وذات أهمية و أولوية عليا. على أن يتناسب مستوى النضوج للنشاطات المتعلقة بأهداف الحاكمية والإدارة وباقي عناصر التمكين السبعة بشكل طردي مع درجة الأهمية والأولوية بحسب نتائج الدراسة المذكورة أعلاه، على أن لا يقل مستوى النضوج للأهداف ذات الأهمية والأولوية العليا عن مستوى 3 Fully Achievedبحسب سلم النضوج الوارد في إطار العمل COBIT 2019، ويسمح باعتبار ما لا يزيد عن 26 % عن الأهداف الواردة في سادسا أعلاه وضمن أهداف الإدارة (بما لا يزيد عن 9 اهداف بحد اقصى من اصل 35 هدف) على أنها ذات أهمية واولوية أدنى اعتمادا على نتائج الدراسة المشار اليها.

- التأكد من وجود إطار عام لإدارة مخاطر تكنولوجيا المعلومات يتوافق ويتكامل مع الإطار العام الكلي لإدارة المخاطر في البنك بحيث يأخذ بعين الاعتبار ويلبي كافة عمليات حاكمية تكنولوجيا المعلومات الواردة في المرفق رقم (3).
- اعتماد موازنة موارد و مشاريع تكنولوجيا المعلومات بما يتوافق والاهداف الاستراتيجية البنك.
- الاشراف العام والاطلاع على سير عمليات و موارد ومشاريع تكنولوجيا المعلومات للتاكد من كفايتها ومساهمها الفاعلة في تحقيق متطلبات وأعمال البنك.

- الاطلاع على تقارير التدقيق لتكنولوجيا المعلومات واتخاذ ما يلزم من إجراءات لمعالجة الانحرافات.
- التوصية لمجلس باتخاذ الإجراءات اللازمة لتصحيح أية انحرافات.
- اعتماد سياسة الأمن السيبراني (Cyber Security Policy).
- اعتماد برنامج الأمن السيبراني(Cyber Security Program)
- فحص الامتثال لسياسة وبرنامج الأمن السيبراني.
- رفع تقرير نصف سنوي إلى مجلس الإدارة عن أعمال وأنشطة اللجنة.
- مراجعة ميثاق اللجنة كل 3 سنوات وأو كلما دعت الحاجة لذلك ورفع أي تعديلات عليه لمجلس الإدارة لاعتماده.
- دراسة أي موضوع يعرض على اللجنة من قبل مجلس الإدارة أو ترى اللجنة ضرورة بحثه وإبداء الرأي والتوصية بشأنه الى مجلس الإدارة.

- **اللجنة التوجيهية لتقنية المعلومات:**

- قامت الإدارة التنفيذية العليا بتشكيل هذه اللجنة وذلك لضمان تطبيق المواءمة الاستراتيجية بين أهداف تكنولوجيا المعلومات لتحقيق الأهداف الاستراتيجية للبنك وبشكل مستدام من خلال تطبيق استراتيجية إدارة تقنية المعلومات المصاغة بالتعاون ما بين إدارة تقنية المعلومات و دائرة الاستراتيجية ، وعليه تم تشكيل لجنة تسمى باللجنة التوجيهية لتكنولوجيا المعلومات برئاسة الرئيس التنفيذي وعضوية مدراء إدارة التنفيذية العليا بما في ذلك المدير التنفيذي لادارة تكنولوجيا المعلومات وإدارة المشاريع والمدير التنفيذي لإدارة المخاطر ومدير دائرة أمن المعلومات ورقابة الجرائم المالية ، وينتخب المجلس أحد أعضائه ليكون عضواً مراقباً في هذه اللجنة بالإضافة للمدير التنفيذي لادارة التدقيق الداخلي، ويمكنها دعوة الغير لدى الحاجة لحضور اجتماعاتها.
- تجتمع هذه اللجنة بشكل ربع سنوي على الأقل، وتحتفظ بسجلات ومحاضر الإجتماع وتوثق حسب الأصول، وتم مراعاة أن تضم هذه اللجنة المهام التاليه:

  - وضع الخطط السنوية المرتبطة بالمعلومات والتكنولوجيا المصاحبة لها والكفيلة بالوصول للأهداف الاستراتيجية المقرة من قبل المجلس.
  - الإشراف على تنفيذ الخطط السنوية لضمان تحقيقها ومراقبة العوامل الداخلية والخارجية المؤثرة عليها بشكل مستمر.
  - ربط أهداف البنك بأهداف المعلومات والتكنولوجيا المصاحبة لها واعتمادها ومراجعتها بشكل مستمر وبما يتضمن تحقيق الأهداف الاستراتيجية للبنك.
  - تعريف مجموعة معايير للقياس (KPI's) ومراجعتها وتكليف المعنيين من الإدارة التنفيذية بمراقبتها بشكل مستمر وإطلاع اللجنة على ذلك.
  - التوصية بتخصيص الموارد المالية وغير المالية اللازمة لتحقيق الأهداف وعمليات حاكمية تكنولوجيا المعلومات
  - الاستعانة بالعنصر البشري الكفوء والمناسب من خلال هياكل تنظيمية تشمل كافة العمليات اللازمة لدعم الأهداف تراعي فصل المهام وعدم تضارب المصالح .
  - الإشراف على سير تنفيذ مشاريع وعمليات حاكمية تكنولوجيا المعلومات.
  - ترتيب مشاريع وبرامج تكنولوجيا المعلومات بحسب الأولوية.
  - مراقبة مستوى الخدمات الفنية والتكنولوجية والعمل على رفع كفاءتها وتحسينها بشكل مستمر.
  - رفع التوصيات اللازمة للجنة حاكمية تكنولوجيا المعلومات بخصوص الأمور التالية:

- تخصيص الموارد اللازمة والآليات الكفيلة بتحقيق مهام لجنة حاكمية تكنولوجيا المعلومات.
- أيه انحرافات قد تؤثر سلبا على تحقيق الأهداف الاستراتيجية.
- أيه مخاطر غير مقبولة متعلقة بتكنولوجيا وأمن وحماية المعلومات.
- تقارير الأداء والامتثال بمتطلبات الإطار العام لإدارة وضبط ومراقبة موارد ومشاريع تكنولوجيا المعلومات.

- تزويد لجنة حاكمية تكنولوجيا المعلومات بمحاضر اجتماعها أولا بأول والحصول على ما يفيد الاطلاع عليها .
- الموافقه على ورفع توصية الى لجنة حاكمية تكنولوجيا المعلومات باعتماد أهمية وترتيب أولوية أهداف المؤسسة (Enterprise Goals)

ومدى ارتباطها بأهداف التوافق (Alignment Goals)
وأهداف الحاكمية والأدارة (Governance and Management Objectives)
بالإضافة لارتباطها بباقي عناصر التمكين (Enablers/Components)
وذلك بناءً على دراسة نوعية و/أو كمية تعد لهذا الغرض بشكل سنوي على الأقل تأخذ بعين الاعتبار العوامل المؤثرة في تشكيل إطار حاكمية تكنولوجيا المعلومات - (COBIT 2019 Design Factors) بما يتناسب مع خصوصية واستراتيجيات البنك، على أن يتم تضمين مواضيع الأمن السيبراني، وإدارة المخاطر وخصوصية وحماية البيانات والامتثال والمراقبة والتدقيق والتوافق الاستراتيجي على أنها Focus Area وذات أهمية وأولوية عليا. على أن يتناسب مستوى النضوج للنشاطات المتعلقة بأهداف الحاكمية والإدارة وباقي عناصر التمكين السبعة بشكل طردي مع درجة الأهمية والأولوية بحسب نتائج الدراسة المذكورة أعلاه، على أن لا يقل مستوى النضوج للأهداف ذات الأهمية والأولوية العليا عن مستوى 3 Fully Achieved بحسب سلم النضوج الوارد في إطار العمل COBIT 2019، ويسمح باعتبار ما لا يزيد عن 26% من الاهداف الواردة في سادسا اعلاه ضمن اهداف الادارة (بما لا يزيد عن 9 اهداف بحد اقصى من اصل 35 هدف) على انها ذات اهمية واولوية ادنى اعتمادا على نتائج الدراسة المشار اليها.

5.7. نظام السياسات:

- على المجلس أو من يُفوّض من لجانه اعتماد منظومة المبادئ والسياسات وأطر العمل اللازمة لتحقيق الإطار العام لإدارة وضبط ومراقبة موارد ومشاريع تكنولوجيا المعلومات وبما يلبي متطلبات الأهداف وعمليات حاكمية تكنولوجيا المعلومات.

- على المجلس أو من يُفوّض 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 الواردة في المرفق رقم أ.

- على المجلس أو من يُفوّض من لجانه اعتماد منظومة السياسات اللازمة لإدارة موارد وعمليات حاكمية تكنولوجيا المعلومات والواردة بالمرفق أ ، واعتبار منظومة السياسات هذه حداً أدنى مع إمكانية الدمج لتلك السياسات حسب ما تقتضيه طبيعة العمل، وعلى أن يتم تطوير سياسات أخرى مواكبة لتطور أهداف البنك وآليات العمل.

- يراعى لدى انشاء السياسات مساهمة كافة الشركاء الداخليين والخارجيين واعتماد أفضل الممارسات الدولية وتحديثاتها كمراجع لصياغة تلك السياسات مثل ISO (COBIT 2019, ISO/IEC 27001/2,
ISO/IEC 38500, ISO/IEC 9126, ISO/IEC 15504, ISO 22301, PCI ,31000
DSS, ITIL, …etc).

5.8. المعلومات والبيانات والتقارير:

- يقوم مجلس الإدارة والإدارة التنفيذية العليا بضمان تطوير البنية التحتية والأنظمة اللازمة لتوفير المعلومات والتقارير لمستخدميها بهدف المساهمة في صنع القرار السليم في البنك.
- يقوم مجلس الإدارة أو الجهات المفوضة بتبني نظم المعلومات والتقارير الواردة في الملحق ب ، وتعتبر هذه الأنظمة الحد الأدنى، ويحدد مالكي هذه المعلومات والتقارير التي يتم من خلالها تحديد سلطة المراجعة والإستخدام وتفويضها حسب الحاجة للعمل.
- يتم مراجعة وتحديث سياسات وتقارير البنك بانتظام وذلك لتعكس أهداف البنك وعملياته وفقا لأفضل الممارسات والمعايير.

5.9. الهيكل التنظيمي:

- 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 عمليات حاكمية تكنولوجيا المعلومات 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.

5.10. الخدمات، والبنية التحتية، والتطبيقات

- على المجلس أو من يُفوّض من لجانه والإدارة التنفيذية العليا اعتماد منظومة الخدمات والبرامج والبنية التحتية الواردة في الملحق ج لتكنولوجيا المعلومات الداعمة والمساعدة لتحقيق عمليات حاكمية تكنولوجيا المعلومات وبالتالي أهداف المعلومات والتكنولوجيا المصاحبة لها، وبالتالي الأهداف المؤسسية.
- على المجلس أو من يُفوّض من لجانه والإدارة التنفيذية العليا اعتماد منظومة الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات، واعتبار تلك المنظومة حداً أدنى، وعلى أن يتم توفيرها و تطويرها بشكل مستمر لمواكبة تطور أهداف وعمليات البنك وبما يتفق وأفضل الممارسات الدولية المقبولة بهذا الخصوص.

5.11. المعرفة، المهارات، والخبرات:

- على المجلس أو من يُفوّض من لجانه اعتماد مصفوفة المؤهلات و سياسات إدارة الموارد البشرية اللازمة لتحقيق متطلبات عمليات حاكمية تكنولوجيا المعلومات ، 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 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 كل بحسب اختصاصه، على أن يتم إعادة تأهيل وتدريب الكوادر الموظفة حالياً لتلبية متطلبات هذا الدليل.
- على الإدارة التنفيذية في البنك الاستمرار برفد موظفيها ببرامج التدريب والتعليم المستمر للحفاظ على مستوى من المعارف والمهارات يلبي ويحقق عمليات حاكمية تكنولوجيا المعلومات.

- على الإدارة التنفيذية في البنك تضمين آليات التقييم السنوي للكوادر بمعايير قياس موضوعية تأخذ بعين الاعتبار المساهمة من خلال المركز الوظيفي بتحقيق أهداف البنك.

5.12. الثقافة، الأخلاقيات والسلوك:

- يعتمد مجلس إدارة البنك أو لجانه المفوضة قواعد السلوك التي تعكس السلوك المهني المتعلق بإدارة المعلومات والتكنولوجيا ذات الصلة التي تحدد بوضوح القواعد والسلوكيات المرغوبة.
- 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 الصادر عن جمعيةISACA : ITAF (Information Technology Assurance Framework) وتحديثاته.
- 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.

5.13. 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 . من خلال كوادر مهنية مؤهلة ومعتمدة دوليابهذا المجال، حاصلين على شهادات اعتماد مهنية سارية مثل CISA
- على لجنة التدقيق المنبثقة عن المجلس من جهة والمدقق الخارجي من جهة أخرى تزويد البنك المركزي الأردني بتقرير سنوي للتدقيق الداخلي و آخر للتدقيق الخارجي على التوالي يتضمن رد الإدارة التنفيذية و إطلاع وتوصيات المجلس بخصوصه، وذلك خلال الربع الأول من كل عام.
- على لجنة التدقيق تضمين مسؤوليات وصلاحيات ونطاق عمل تدقيق تكنولوجيا المعلومات ضمن ميثاق التدقيق من جهة وضمن اجراءات متفق عليها مع المدقق الخارجي من جهة أخرى.
- على المجلس التأكد ومن خلال لجنة التدقيق المنبثقة عنه من قيام المدقق الداخلي و المدقق الخارجي للبنك لدى تنفيذ عمليات التدقيق المتخصص للمعلومات والتكنولوجيا المصاحبة لهاالإلتزام بما يلي:
  - معايير تدقيق تكنولوجيا المعلومات بحسب أخر تحديث للمعيار الدولي ITAF الصادرعنجمعية التدقيق والرقابه ISACAومنها:
    - 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 وضمان عدم تضارب المصالح.
    - الإلتزام بمعايير الموضوعية وبذل العناية المهنية والحفاظ المستمر على مستوى التنافسية والمهنية .

- فحص وتقييم ومراجعة عمليات توظيف وإدارة موارد تكنولوجيا المعلومات وعمليات البنك المرتكزة عليها واعطاء رأي عام حيال مستوى المخاطر الكلي للمعلومات والتكنولوجيا المصاحبة لها ضمن برنامج تدقيق.
- 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.
- تضمين آليات التقييم السنوي 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، أو من يحل محلها في البنوك الأجنبية.
- من الممكن إسناد دور المدقق الداخلي للمعلومات والتكنولوجيا المصاحبة لها لجهة خارجية متخصصة مستقلة تماما عن المدقق الخارجي المعتمد بهذا الخصوص، شريطة تلبية كافة متطلبات هذه التعليمات وأية تعليمات أخرى ذات صلة و احتفاظ لجنة التدقيق المنبثقة عن المجلس والمجلس نفسه بدورهما فيما يتعلق بفحص الامتثال والتأكد من تلبية هذه المتطلبات كحد أدنى.

6. وضع الأهداف وتتابعها

تعمل كل مؤسسة في سياق مختلف عن الأخرى ويتم تحديد هذا السياق بواسطة عوامل خارجية وأخرى داخلية. فالعوامل الخارجية تتضمن السوق، الصناعة، السياسات الجغرافية، الخ؛ أما العوامل الداخلية فتشمل الثقافة، التنظيم، القابلية للمخاطرة، الخ. ويتطلب هذا السياق المؤسسي نظاما للحوكمة والإدارة يتناسب معه.

يجب أن يتم تحويل إحتياجات أصحاب المصلحة إلى إسترتيجية مؤسسية قابلة للتنفيذ تشكل أهداف كوبت المتكاملة آلية لترجمة إحتياجات أصحاب المصلحة إلى أهداف مؤسسية مجدية قابلة للتنفيذ يتم تخصيصها وفقا للمطلوب، ويستنبط منها أهداف التوافق. إن هذه الترجمة تتيح وضع أهداف محددة على كل مستوى وفي كل مجال في المؤسسة لدعم الأهداف الشاملة ومتطلبات أصحاب المصلحة وبذلك يتم الموائمة بين إحتياجات البنك وحلول وخدمات تقنية المعلومات ودعمها بشكل فاعل.

وقد اعتمد البنك آلية كوبيت للأهداف المتتالية لترجمة احتياجات أصحاب المصلحة إلى أهداف محددة وقابلة للتنفيذ ومخصصة لأعمال وأهداف تتعلق بأهداف التوافق وأهداف تمكينية. وتتيح هذه الترجمة وضع أهداف محددة على كل مستوى وفي كل مجال من مجالات البنك لدعم الأهداف العامة ومتطلبات أصحاب المصلحة، وبالتالي تدعم بشكل فعال المواءمة بين احتياجات البنك وحلول وخدمات تكنولوجيا المعلومات.

الملحق أ : منظومة السياسات(حد أدنى)

** يستند الجدول أدناه إلى تعليمات البنك المركزي الأردني ملحق رقم (6)*

يعتمد البنك القائمة التالية من الحد الأدنى من السياسات لتنظيم وإدارة العمليات في البنك.

اسم السياسة	الغرض	النطاق
حاكمية تنظيم تكنولوجيا المعلومات	وضع القواعد والمعايير اللازمة لإدارة موارد تكنولوجيا المعلومات بما في ذلك الشكل الإداري (مركزي أو لا مركزي)، والهياكل التنظيمية بما في ذلك النشاطات والمهام والمسؤوليات لإدارة تلك الموارد بما في ذلك الموارد المالية.	عمليات وخدمات ومشاريع تكنولوجيا المعلومات.
أمن وحماية المعلومات	وضع القواعد والمعايير اللازمة لضمان متطلبات الحماية والسرية والمصداقية والتوافرية والامتثال لإدارة موارد تكنولوجيا المعلومات بحسب المعايير الدولية المقبولة بهذا الخصوص مثل ISO-IEC (27001/2	كافة المعلومات والتكنولوجيا المصاحبة لها.
خطط استمرارية العمل وخطط التعافي من الكوارث.	وضع القواعد والمعايير اللازمة لبناء خطط التعافي من الكوارث وحماية البشر، وخطط استمرارية العمل بما في ذلك آليات بناء وتشغيل وفحص والتدريب على وتحديث تلك الخطط لضمان توافرية عمليات البنك الحرجة.	عمليات البنك الحرجة، وحماية البشر.
إدارة مخاطر تكنولوجيا المعلومات	وضع القواعد والمعايير اللازمة لإدارة مخاطر تكنولوجيا المعلومات على اعتبارها جزء من المخاطر الكلية للبنك، بما في ذلك حاكمية تلك المخاطر والمسؤوليات والمهام المناطة بالأطراف المختلفة، وآليات تقييم وضبط ومراقبة المخاطر، بهدف تعزيز عمليات اتخاذ القرار المبني على المخاطر وتحقيق أهداف البنك.	كافة عمليات البنك ومدخلاتها الخاصة بتكنولوجيا المعلومات.
(ITالامتثال (Compliance	وضع القواعد والمعايير اللازمة لضمان الامتثال لتعليمات البنك المركزي والجهات الرقابية الأخرى وللقوانين والأنظمة السارية ولسياسات البنك.	كافة عمليات البنك بمواضيع تكنولوجيا المعلومات.
(Dataخصوصية البيانات (Privacy	وضع القواعد والمعايير اللازمة لحماية البيانات الخاصة المتعلقة بأفراد طبيعيين أو اعتباريين من عمليات الافصاح والاستخدام غير المصرح به.	كافة البيانات الخاصة.
(Outsourcing)التعهيد	اعتماد سياسة عامة للاستعانة بالموارد بشكل عام وبموارد تكنولوجيا المعلومات بشكل خاص، تلك أو (In-sourcing) الموارد سواء المملوكة للبنك تراعي (Outsourcing) المملوكة للغير التعليمات والأنظمة والقوانين وتحاكي أفضل الممارسات الدولية المقبولة بهذا الخصوص، وتأخذ بعين الاعتبار مكان العملية الإنتاجية On-site ، (Off-site, Near-site, Off-shore و تأخذ بعين الاعتبار وتراعي متطلبات مراقبة مستوى وتفعيل حق التدقيق (Service Levels) الخدمات من قبل أطراف ثالثة محايدة(Audit Right) موثوقة، وتحقيق متطلبات استمرارية العمل وضوابط الحماية اللازمة لتلبية متطلبات السرية والمصداقية بالإضافة لمتطلبات الكفاءة والفعالية في استغلال الموارد..	كافة عمليات البنك.
(Project)إدارة المشاريع Portfolio (Management	وضع القواعد والمعايير اللازمة لإدارة المشاريع بما في ذلك مراحل المشروع وحاكميته اللازمة لتحقيق (Quality)المتطلبات المتعلقة بالجودة وتلك المتعلقة بالحماية والسرية (Requirements وتلك(Confidentiality Requirements) المتعلقة بالامتثال تحقيقا لأهداف البنك وعملياته.	كافة مشاريع البنك المتعلقة بتكنولوجيا المعلومات.
(Asset إدارة الموجودات	وضع القواعد والمعايير اللازمة لتصنيف درجة مخاطر البيانات والأنظمة المختلفة، وتحديد مالكيه وضوابط حمايتها خلال مراحل دورة حياتها المختلفة.	البيانات والأجهزة والبرامج

اسم السياسة	الغرض	النطاق
(Management		والأدوات المصاحبة لها.
الاستخدام المقبول لموارد تكنولوجيا المعلومات	وضع القواعد والمعايير اللازمة لتحديد السلوك المقبول وغير المقبول لموارد تكنولوجيا المعلومات.	الأجهزة والبرمجيات والتطبيقات والشبكات بما في ذلك الإنترنت والبريد الإلكتروني.
إدارة التغيير (Change Management)	وضع القواعد والمعايير اللازمة لضمان مصداقية التغيير من حيث توثيق الموافقات اللازمة من مالكي الأصول الخاضعة للتغيير.	كافة عمليات تكنولوجيا المعلومات.
أجهزة الكمبيوتر المركزية	وضع قواعد ومعايير لتقليل عمليات النفاذ والاستخدام غير المشروع للأجهزة بما في ذلك ضوابط نفاذ موظفي دائرة تكنولوجيا المعلومات وذوي الامتيازات العليا لبيئات التشغيل، بالإضافة لمعايير إدارة عمليات التشغيل اليومي للأجهزة والبر مجيات المختلفة بما في ذلك ضوابط الحماية وآليات المراقبة والصيانة الدورية لتلك الأجهزة.	كافة الأجهزة المركزية المملوكة أو المدارة من قبل البنك لكافة بيئات التطوير والفحص والتشغيل، بما في ذلك نظم التشغيل والأدوات الأخرى المصاحبة لها.
أجهزة الكمبيوتر الطرفية	وضع قواعد ومعايير سلوك وأخرى تقنية لضمان حماية البيانات الحساسة المخزنة على الأجهزة.	كافة الأجهزة الطرفية المرتبطة بالشبكات أو القائمة بحد ذاتها.
الأجهزة المحمولة	وضع قواعد ومعايير سلوك وأخرى تقنية لضمان حماية البيانات الحساسة المخزنة على الأجهزة.	كافة الأجهزة المحمولة مثل (Laptop, PDA, Smart Phone, USB Memory Cards, ...etc)
إدارة صلاحيات وامتيازات النفاذ (User Access Management)	وضع قواعد ومعايير لضمان منح صلاحيات وامتيازات النفاذ للبيانات والبرامج والأجهزة لمستخدميها بحسب الحاجة للعمل وبالحد الأدنى بما يكفل السرية والمصداقية والتوافرية لموارد تكنولوجيا المعلومات.	كافة البرامج والأجهزة وقواعد البيانات وما هو في حكمها.
سياسة تطوير / اقتناء البرمجيات (System Development Life Cycle)	وضع القواعد والمعايير اللازمة لتنفيذ مراحل تطوير /اقتناء البرمجيات المختلفة لضمان تلبيتها لمتطلبات العمل من خلال منهجيات التطوير المختلفة المتناسبة مع متطلبات وأهداف العمل.	البرمجيات الجديدة والقديمة المطورة محليا والمقتناة من مصادر خارجية.
إدارة مستوى الخدمات (Service Level Management)	وضع قواعد ومعايير لتحديد وقبول وتوثيق وقياس ومراقبة وتحسين مستوى الخدمات المقدمة سواء من أطراف داخلية أو أطراف خارجية لضمان الاستغلال الأمثل للموارد ودعم عمليات البنك المختلفة.	كافة الاتفاقيات والتعاقدات والإلتزامات مع الأطراف الخارجيين والأطراف من داخل البنك.
النسخ الاحتياطي والاسترجاع (Back-up and Restore)	وضع قواعد ومعايير لآليات النسخ الاحتياطي والاسترجاع لضمان توافرية البيانات ومصداقيتها وسريتها.	البيانات في بيئات التشغيل وحيثما يلزم.

اسم السياسة	الغرض	النطاق
الاحتفاظ بالبيانات (Retention)	وضع القواعد والمعايير الخاصة بحجم البيانات الواجب تو افرها سواء بشكل ورقي أو تلك المتواجدة (On-على أجهزة الكمبيوتر والتطبيقات المختلفة والمدة الزمنية الواجب الاحتفاظ بهاLine Data) والمفاضلة بين حجم البيانات المتو افرة والسرعة والأداء في الوصول إلى البيانات.	كافة الأجهزة والبرمجيات ووسائل وأدوات الاحتفاظ بالبيانات.
شراء الأنظمة والتجهيزات (Purchasing)	وضع قواعد ومعايير للمفاضلة بين المزودين الخارجيين.	كافة التجهيزات التقنية والبرامج المتعلقة بها.
النفاذ عن بعد (Remote Access)	وضع قواعد ومعايير للربط الشبكي عن بعد بشبكات الكمبيوتر الخاصة بالبنك، لتقليل مخاطر الاطلاع والاستخدام لبيانات ومصادر البنك الحساسة ولأنظمة الضبط والرقابة الداخلية المعنية بحماية موجودات البنك، وللحماية من مخاطر السمعة.	الأطراف والشركاء الداخليين والخارجيين مثل مزودي الخدمات، ولكافة بيئات التطوير والفحص والتشغيل للأجهزة والشبكات، ومنها على سبيل المثال لا الحصر شبكات الإنترنت، والشبكات المشفرة، وخطوط الاتصال المختلفة مثل (VPN, Frame relay, ISDN, DSL, MPLS).
الشبكا(Networks)	وضع قواعد ومعايير لضمان تحقيق متطلبات الكفاءة والفعالية في استغلال عناصر الشبكات والاتصالات من جهة وتحقيق متطلبات الأمن والحماية من جهة أخرى دعما لتحقيق أهداف البنك.	كافة عناصر الشبكات بكافة البيئات.
الشبكات اللاسلكية (Wireless Networks)	وضع قواعد ومعايير بغرض حماية البيانات الحساسة المتناقلة عبر الشبكات اللاسلكية من الاعتراض والاستخدام غير المشروع.	كافة الشبكات اللاسلكية الفعلية منها والافتراضية.
أجهزة الحماية (Firewalls)	وضع الحد الأدنى من القواعد و المعايير الناظمة لتفعيلها (Firewalls) لآلية عمل وحماية أجهزة بالشكل المطلوب الكفيل بحماية وضمان سرية ومصداقية بيانات وعمليات البنك وتوافريتها.	(Firewalls)كافة أجهزة ال العاملة بكافة البيئات مثل DMZ, Proxy, External) DNS, VPN, Routers, (Switches, Servers, …etc.
فحص الإختراق وتحليل الثغرات Penetration) Testing and Vulnerability (Assessment	وضع قواعد ومعايير لفحص الأجهزة وعناصر الشبكات لضمان عدم وجود ثغرات أمنية تمكن من اختراق البيانات والأنظمة والعمليات الحساسة للبنك.	كافة موجودات البنك التقنية من أجهزة كمبيوتر مركزية وأجهزة طرفية وأجهزة حماية وعناصر شبكات وبرمجيات.
(مقسم الهاتف (Public Branch Exchange)	وضع الحد الأدنى من قواعد ومعايير الحماية لأنظمة المقسم لضمان الحماية والسرية لبيانات وعمليات البنك من الاستخدام غير المشروع.	كافة أجهزة المقسم المملوكة وغير المملوكة للبنك.

الملحق ب: الحد الأدنى من التقارير والمعلومات

** يستند الجدول أدناه إلى تعليمات البنك المركزي الأردني ملحق رقم 7*

سيعتمد البنك قائمة الحد الأدنى من التقارير الواردة أدناه لضمان المحافظة على التقارير السليمة في البنك، وتعتبر التقارير بمثابة مرساة لعمليات صنع القرار.

1. مصفوفة الصلاحيات والامتيازات
2. تحليل عوامل المخاطر
3. سيناريو تحليل مخاطر تكنولوجيا المعلومات
4. سجل مخاطر تكنولوجيا المعلومات
5. جدول المسؤوليات لكل خدمة مقدمةRACI Chart
6. ملف مخاطر تكنولوجيا المعلومات
7. تقرير مخاطر تكنولوجيا المعلومات
8. خريطة مخاطر تكنولوجيا المعلومات
9. Risk Universe, Appetite and Tolerance
10. مؤشرات المخاطر الرئيسية
11. Risk Taxonomy
12. Risk and Control Activity Matrix (RCAM)
13. موازنة أمن وحماية المعلومات
14. MIS Report
15. استراتيجية أو منهجية تدقيق تكنولوجيا المعلومات
16. ميثاق التدقيق
17. خطة تدقيق تكنولوجيا المعلومات
18. مصفوفة المؤهلات
19. سجل تدقيق تكنولوجيا المعلومات
20. ملف تدقيق تكنولوجيا المعلومات
21. أفضل المعايير الدولية لإدارة موارد ومشاريع تكنولوجيا المعلومات، وإدارة مخاطر تكنولوجيا المعلومات، وأمن وحماية والتدقيق على تكنولوجيا المعلومات

الملحق ج: الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات

سيعتمد البنك قائمة الأنظمة والخدمات والبنية التحتية لتكنولوجيا المعلومات التي تدعم المعلومات التالية لتحقيق عمليات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها.

1. خدمات إدارة الحوادث
2. جرد أصول تكنولوجيا المعلومات
3. التوعية بالممارسات الجيدة لأمن المعلومات
4. أمن وحماية البيانات والمعلومات المنطقي
5. المراقبة لأمن المعلومات
6. برمجيات تدقيق تكنولوجيا المعلومات
7. مراقبة الأمن المادي والبيئي لغرف الخوادم وغرف الاتصالات والإمداد بالكهرباء.

التعريفات

- **الحاكمية**: تضمن الحاكمية تقييم احتياجات أصحاب المصلحة وشروطهم وخياراتهم من أجل تحديد أهداف متوازنة ومتفق عليها على مستوى المؤسسة يتم تحقيقها؛ وتحديد التوجهات المؤسسية من خلال تحديد الأولويات واتخاذ القرارات؛ ورصد الأداء والامتثال اتجاه الاهداف المتفق عليها.
- **كوبت**: تعرف سابقا بأهداف الرقابة على المعلومات والتكنولوجيا ذات الصلة كوبيت ؛ وتستخدم الآن فقط الان كإسم.
- إطار كامل ومقبول دوليا لحوكمة وإدارة معلومات المؤسسة والتكنولوجيا التي تدعم المدراء التنفيذيين في المؤسسة والإدارة في تعريفها وتحقيق أهداف العمل وأهداف التوافق ذات الصلة. يدعم كوبت المؤسسات في تطوير وتنفيذ وتحسين ومراقبة ممارسات الحاكمية والإدارة الجيدة المتعلقة بتكنولوجيا المعلومات.
- **هدف المؤسسة**: هدف العمل.
- **حوكمة التكنولوجيا والمعلومات في المؤسسة**: رؤية للحوكمة تضمن المعلومات ودعم التكنولوجيا ذات الصلة وتساهم في تحقيق أهداف المؤسسة.
- **مجلس الإدارة**: مجلس إدارة البنك.
- **الإدارة التنفيذية العليا**: تشمل الرئيس التنفيذي للبنك أو المدير الإقليمي، نائب الرئيس التنفيذي أو نائب المدير الإقليمي، مساعد الرئيس التنفيذي أو المدير الإقليمي المساعد، المدير المالي، مدير العمليات، مدير إدارة المخاطر، رئيس الخزانة (الاستثمار)، مدير الامتثال، وكذلك أي موظف في البنك يتمتع بسلطة تنفيذية موازية لأي من السلطات المذكورة أعلاه، ويرتبط وظيفيا ومباشرة بالمدير العام.
- **أصحاب المصلحة**: أي طرف معني في البنك، مثل المساهمين أو الموظفين أو الدائنين أو العملاء أو الموردين أو الهيئات التنظيمية الخارجية المعنية.
- **المدقق**: الشخص (الطبيعي أو المعنوي) أو الجهه المختصه بفحص عمليات البنك المرتكزه على تكنولوجيا المعلومات وبما ينسجم مع متطلبات التعليمات بهذا الخصوص و المتفق معه من قبل اداره البنك لتحقيق تلك المتطلبات لفتره لا تقل عن 3 سنوات متتاليه و لا تزيد عن 6 سنوات متتاليه.