

دليل حاكمية وإدارة المعلومات
والتكنولوجيا المصاحبة لها

2021

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

| رقم النسخة | التاريخ |
|------------|-------------------|
| 01 | April 10, 2017 |
| 02 | June 17, 2019 |
| 03 | November 16, 2020 |
| 04 | June 15, 2021 |

قائمة المحتويات

| | |
|----|--|
| 4 | 1. المقدمة |
| 4 | 2. ملحة عامة عن بنك الإستثمار العربي الأردني |
| 5 | 3. النطاق |
| 6 | 4. الأهداف |
| 6 | 5. السياسات العامة |
| 9 | 6. المبادئ الستة لنظام الحاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها |
| 9 | 7. وضع الأهداف وتتابعها |
| 11 | الملحق أ: منظومة السياسات (حد أدنى) |
| 16 | الملحق ب: الحد الأدنى من التقارير والمعلومات |
| 17 | الملحق ج: الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات |
| 18 | الملحق د: التعريفات |
| 19 | المصادر والمراجع |

1. المقدمة

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

وإستجابة لتعليمات البنك المركزي الأردني رقم 2016/65 و تعميم رقم (10-6-984). قام بنك الاستثمار العربي الأردني بالمبادرة لإعتماد إطار كويت لحاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها إمتثالاً للتعليمات الصادرة بهذا الخصوص.

يوفر كويت إطار شامل يساعد بنك الاستثمار العربي الأردني في تحقيق أهدافه المتعلقة بحاكمية وإدارة تكنولوجيا المعلومات على مستوى البنك بشكل كامل. حيث أن هذا الإطار يساعد البنك على الوصول إلى أعلى درجات الفائدة من تكنولوجيا المعلومات من خلال الحفاظ على التوازن بين الحصول على أعلى فائدة من تكنولوجيا المعلومات وبأقل المخاطر والموارد.

يمكن الإطار كويت تكنولوجيا المعلومات من التطبيق الكلي للحاكمية وإدارة لكافة وحدات الأعمال في بنك الاستثمار العربي الأردني. أي بمعنى آخر تغطية لكافة الأعمال ووظائف تكنولوجيا المعلومات ومسؤولياتها في البنك.

2. ملحة عامة عن بنك الاستثمار العربي الأردني

منذ أربعة عقود، بدأ بنك الاستثمار العربي الأردني (AJIB) مسيرة حافلة من التميز والريادة ليتبوأ اليوم مكانة بارزة كواحد من أهم البنوك الاستثمارية والتجارية في الأردن. وانطلاقاً من التزامه بتحقيق رضا العملاء وتلبية كافة احتياجاتهم، يحرص البنك على توفير مجموعة من الخدمات المبتكرة والمنتجات الرائدة التي من شأنها تلبية جميع الاحتياجات المصرفية الاستثمارية منها والتجارية. يلتزم بنك الاستثمار العربي الأردني بتطوير موارده البشرية وتحديثها والارتقاء بها بشكل مستمر كما يسعى إلى تعزيز الموارد البشرية وتوفير أحدث التقنيات وأفضل الممارسات وآليات العمل؛ وذلك استجابة للاحتياجات المتنامية لعملائه من الشركات والأفراد ذوي الملاة الائتمانية والمالية العالية في الأردن والمنطقة.

يقوم البنك اليوم بدور حيوي وهام في واقع الاستثمار المصرفي في المنطقة. ويعود ذلك إلى الخبرات والكفاءات العالية التي يمتاز بها البنك في مجال الاستثمار المصرفي وما يقدمه من منتجات وحلول مبتكرة للشركات في هذا المجال. يحرص بنك الاستثمار العربي الأردني بتقديم سلسلة واسعة من الخدمات المصرفية والاستثمارية المتكاملة بما في ذلك دمج الشركات وتملك الأصول والأنشطة الخاصة بأسواق الأسهم (السوق الرئيسي والثانوي)، إلى جانب تقديم الخدمات الاستثمارية في التعاملات والأبحاث المتعلقة بالأسهم والأسواق ومنح القروض بكافة أنواعها للشركات وتمويل المشاريع. ومن جهتها، تواصل دائرة خدمات ومبيعات الأفراد مساعيها وجهودها الرامية إلى توفير منتجات وخدمات متنوعة في مجالات القروض الشخصية والسكنية ومختلف أنواع البطاقات الائتمانية وغيرها من الخدمات المبتكرة.

يرحب بنك الإستثمار العربي الأردني بعملائه الكرام من خلال شبكة فروع المنتشرة في مواقع رئيسية في المملكة الأردنية الهاشمية. يصاحبها شبكة متطورة من أجهزة الصراف الآلي والتي تشكل جزءاً من الشبكة الوطنية التي تشمل على ما يزيد عن ألف صراف آلي (JONET).

تتجسد فلسفة البنك في السعي الدائم نحو تحقيق رضا العميل في المقام الأول. وقد أثمرت هذه الفلسفة التي تقوم على الالتزام والتخطيط المسبق عن مبادئ راسخة مكنتنا من تحقيق أداء مالي قوي وانتهاج سياسات استثمارية متزنة وناجعة. هدفنا هو ضمان توفير حلول استثمارية ومصرفية تتناسب مع احتياجات العملاء تعتمد على دراسات تحليل الأسواق التي يجريها البنك بشكل منتظم.

يولي بنك الإستثمار العربي الأردني (AJIB) أهمية بالغة للموظفين الذين يشكلون العنصر الأهم والأعلى قيمة في هذه المؤسسة؛ وفي ضوء ذلك يحرص البنك على توفير بيئة عمل صحية ومواتية تتيح لهم فرصة النمو والازدهار وتحقيق أقصى إمكاناتهم. يؤمن بنك الإستثمار العربي الأردني (AJIB) بقوة المعرفة والتكنولوجيا والمهارات على أن تكون مدعومة بما يلزم من حكمة ونفاد بصيرة وقدرة على التخطيط للمستقبل.

يسعى بنك الإستثمار العربي الأردني (AJIB) إلى أن يصبح واحداً من البنوك الاستثمارية والتجارية الرائدة التي تحظى بأفق رحب من الكفاءات العالية والتقنيات الحديثة التي تهدف إلى منح العميل تجربة فريدة من نوعها وتحقيق أعلى قيمة من حقوق المساهمين.

3. النطاق

ينطبق هذا الدليل على كافة عمليات بنك الإستثمار العربي الأردني التي تعتمد على تكنولوجيا المعلومات بكافة دوائر وفروع البنك. يجب على كافة أصحاب المصالح مراعاة الإمتثال لهذه التعليمات وكل حسب مسماه وموقعة الوظيفي.

القائمة أدناه تمثل الأطراف الرئيسية ومسؤولياتها بهذا الخصوص:

- رئيس وأعضاء المجلس والخبراء الخارجيين المستعان بهم: تولي مسؤوليات التوجيه العام للمشروع / البرنامج والموافقة على المهام والمسؤوليات ضمن المشروع. والدعم وتقديم التمويل اللازم.
- وفقاً لتعليمات البنك المركزي الأردني. يتحمل مجلس إدارة بنك الإستثمار العربي الأردني المسؤولية المباشرة لعمليات الحوكمة (التقييم والتوجيه والمراقبة).
- يتولى مجلس إدارة بنك الإستثمار العربي الأردني وإدارة المخاطر المسؤولية المباشرة عن عملية ضمان تقليل المخاطر وعملية إدارة المخاطر وعناصر التمكين المرتبطة بها.
- المدير العام ونوابه ومساعديه ومدراء العمليات 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. والمشاركة في المشروع / البرنامج بما يمثل دور التدقيق الداخلي في الأمور التنفيذية كمستشار ومراقب مستقل لتسهيل وإنجاح إتمام المشروع / البرنامج.

- إدارات المخاطر وأمن المعلومات والامتثال والقانونية: تولي مسؤوليات المشاركة في المشروع /البرنامج بما يمثل دور تلك الإدارات، والتأكد من تمثيل المشروع/البرنامج من قبل كافة الأطراف المعنية المتخصصين وحملة الشهادات الفنية والمهنية الخاصة بالمعيار.

4. الأهداف

وضع بنك الإستثمار العربي الأردني الأهداف التالية لإطار حاكمية وإدارة المعلومات والتكنولوجيا المصاحبه لها:

4.1. تلبية احتياجات أصحاب المصلحة وتحقيق أهداف البنك من خلال استخدام إطار حوكمة راسخ النضوج.

- تسهيل الوصول إلى القيمة المطلوبة من خلال تقديم الفوائد والنتائج المتوقعة، وتحسين مستوى المخاطر وتحسين إستغلال الموارد.

- توفير معلومات ذات جودة عالية كمرتكز يدعم آليات صنع القرار في البنك.

- ضمان توفير البنية التحتية التكنولوجية التي تمكن البنك من تحقيق أهدافه.

- ضمان رفع مستوى العمليات المصرفية وذلك من خلال استخدام وتوظيف أنظمة تكنولوجية فعالة وموثوق بها وأن يتم إختيارها لتحقيق الأهداف المنشودة.

- ضمان توفير إدارة مخاطر تكنولوجيا المعلومات بشكل صارم لضمان الحماية الضرورية واللازمة لأصول البنك.

- توفير المساعدة في تحقيق الإلتزام بمتطلبات القوانين واللوائح والتعليمات وكذلك الإلتزام بسياسات البنك واستراتيجيته وإجراءات العمل المعمول بها داخليا.

- تحسين نظام الضبط والرقابة الداخلي.

- تعظيم مستوى رضا مستخدمي تكنولوجيا المعلومات من خلال تلبية احتياجات عملهم بكفاءة وفعالية.

- إدارة خدمات العملاء والأطراف الخارجية المكلفة بتنفيذ العمليات والخدمات والمنتجات.

4.2. فصل مجلس الإدارة عن الإدارة التنفيذية بما يتوافق وأفضل المعايير والممارسات المعترف بها دوليا لحاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها.

5. السياسات العامة

5.1. يستند هذا الدليل إلى تعليمات البنك المركزي الأردني رقم: 2016/65 و تعميم رقم (10-6-984) ، والتي جاءت إعتقادا على إطار كويت. وينبغي مراجعة وتحديث هذا الدليل سنويا أو عند الحاجة وبما يتواءم مع التحديثات التي تطرأ على مستوى اللوائح وتحديثات الإطار كويت التي تصدر من قبل جمعية التدقيق والرقابة على نظم المعلومات ISACA.

5.2. يقوم البنك، من خلال لجنة حاكمية تكنولوجيا المعلومات المنبثقة عن مجلس الإدارة، بمراجعة هذا الدليل وتحديثه عند الضرورة.

5.3. يقوم البنك، بنشر هذا الدليل على الموقع الإلكتروني للبنك ومن خلال أي طريقة مناسبة متاحة للعوام.

5.4. اللجان

- قام البنك بتشكيل اللجان اللازمة لتنظيم وتوجيه إطار الحاكمية في البنك. حيث تم تشكيل لجنة حاكمية تكنولوجيا المعلومات واللجنة التوجيهية لتكنولوجيا المعلومات.
- 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 الأقل، وتضم في عضويتها أهل الخبرة والمعرفة في تكنولوجيا المعلومات.
- تجتمع هذه اللجنة بشكل ربع سنوي على الأقل. ويتم الإحتفاظ بسجلات ومحاضر الإجتماع وتوثق حسب الأصول. وتم مراعاة أن تضم هذه اللجنة المهام المذكورة في لوائح وتعليمات البنك المركزي الأردني.
- اللجنة التوجيهية لتكنولوجيا المعلومات:
- قامت الإدارة التنفيذية العليا بتشكيل هذه اللجنة وذلك لضمان تطبيق الموازنة الاستراتيجية بين أهداف التوافق والأهداف الاستراتيجية للبنك. ويرأس هذه اللجنة المدير العام وتضم في عضويتها كبار المدراء التنفيذيين. بما في ذلك مدير تكنولوجيا و أمن المعلومات، مدير إدارة المخاطر. بالإضافة إلى وجود عضو مراقب من أعضاء مجلس الإدارة وفقا لمتطلبات البنك المركزي الأردني وكذلك مدير التدقيق الداخلي. ويحق للجنة دعوة أطراف أخرى لحضور الاجتماعات عند الحاجة.
- تجتمع هذه اللجنة بشكل ربع سنوي على الأقل. ويتم الإحتفاظ بسجلات ومحاضر الإجتماع وتوثق حسب الأصول. وتم مراعاة أن تضم هذه اللجنة المهام المذكورة في لوائح وتعليمات البنك المركزي الأردني.

5.5. عمليات البنك وتكنولوجيا المعلومات وأهدافها المرتبطة:

تتولى لجنة حاكمية تكنولوجيا المعلومات:

- اعتماد 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.

5.6. نظام السياسات:

يعتمد مجلس الإدارة أو لجانه المختصة نظام السياسات اللازمة لإدارة وتشغيل حاكمية تكنولوجيا المعلومات كما هو مبين في الملحق أ ويعتبر هذا النظام للسياسات هو الحد الأدنى مع إمكانية دمج هذه السياسات مع غيرها وفقا لما تتطلبه طبيعة العمل.

5.7. 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.
- توفر أهداف المعلومات ومعايير الجودة إرشادات لإدارة المعلومات وفقا لاستخدامها.
- 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.

5.8. الهيكل التنظيمي:

- يعتمد مجلس الإدارة الهياكل التنظيمية (الهيكل الهرمي وهياكل اللجان) فيما يتعلق بإدارة الموارد والعمليات والمشاريع الخاصة بتكنولوجيا المعلومات وإدارة المخاطر وتكنولوجيا المعلومات وأمن المعلومات وإدارة الموارد البشرية التي تلبى المتطلبات التشغيلية للحاكمية، وإدارة تكنولوجيا المعلومات، وتحقيق أهداف البنك بكفاءة وفعالية.

5.9. الخدمات، والبنية التحتية، والتطبيقات

- سيقوم البنك مثلا بمجلس الإدارة وإدارته التنفيذية بتبني نظام الخدمات، والبنية التحتية، والتطبيقات الوارد في الملحق ج ذلك للوصول إلى خدمات الحاكمية وأهداف التوافق وبالتالي أهداف البنك بشكل عام.

5.10. المعرفة، المهارات، والخبرات:

- تقوم إدارة البنك ومجلس الإدارة أو اللجان المفوضة باعتماد المصفوفات اللازمة (كفاءات الموارد البشرية) وسياسات إدارة الموارد البشرية لتحقيق متطلبات حاكمية تكنولوجيا المعلومات وضمن وجود الموارد البشرية المناسبة.
- تقوم الإدارة التنفيذية للبنك بتسجيل موظفيها في برامج التدريب والتعليم المستمر للحفاظ على مستوى المعرفة والمهارات اللازمة للوفاء بحاكمية تكنولوجيا المعلومات وتحقيقها.

5.11. 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.

إطار حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها

6. المبادئ الستة لنظام الحاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها

يستند إطار حاكمية المعلومات والتكنولوجيا المصاحبة لها في بنك الإستثمار العربي الأردني إلى ستة مبادئ رئيسية لنظام كوبيت 2019:

1. تحقيق القيمة المرجوة التي تلبي احتياجات أصحاب المصالح من خلال الحفاظ على التوازن بين التعامل الأمثل مع المخاطر، والاستخدام الأمثل للموارد، وتحقيق القيمة.
2. الفصل بين مسؤوليات الحاكمية والإدارة من خلال توزيع الأدوار والمسؤوليات في كل المستويات واللجان ذات الصلة.
3. التغطية الشاملة للبنك.
4. تطبيق إطار عمل صُمِّمَ وتمَّ تكيفه ليلبي احتياجات البنك، وذلك من خلال استخدام مجموعة من العناصر التي تأخذ بعين الاعتبار العوامل المؤثرة في تشكيل إطار حاكمية تكنولوجيا المعلومات (COBIT 2019 - Design Factors) بما يتناسب مع خصوصية واستراتيجيات البنك. لترتيب أهمية وألوية أهداف إدارة وحاكمية التكنولوجيا والمعلومات المصاحبة لها في البنك.
5. تطبيق إطار عمل ديناميكي قابل للتحديث والتطوير لمواكبة التغيرات في المؤسسة. ففي حال تغير أي من عوامل تصميم هذا الإطار (على سبيل المثال تغير في استراتيجية المؤسسة أو التكنولوجيا) يمكن النظر في تأثير هذه التغيرات على نظام الحاكمية في البنك و تحديثه لمواكبة واستيعاب هذه التغيرات وتلبية الاحتياجات الجديدة.
6. تطبيق منهجية شاملة لحاكمية وإدارة تكنولوجيا المعلومات من خلال 7 عناصر تمكين وهي:
 - المبادئ والسياسات وأطر العمل.
 - عمليات حاكمية تكنولوجيا المعلومات.
 - الهياكل التنظيمية.
 - المعلومات والتقارير.
 - الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات.
 - المعارف والمهارات والخبرات.
 - منظومة القيم والأخلاق والسلوكيات

7. وضع الأهداف وتتابعها

تعمل كل مؤسسة في سياق مختلف عن الآخر 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 استراتيجية مؤسسية قابلة للتنفيذ. تشكل أهداف كويت 2019 المتكاملة آلية لترجمة إحتياجات أصحاب المصلحة إلى أهداف مؤسسية مجدية قابلة للتنفيذ يتم تخصيصها وفقا للمطلوب. ويستنبط منها أهداف التوافق وأهداف عمليات ادارة و حاكمية وعناصر التمكين المرتبطة بها. إن هذه الترجمة تتيح وضع أهداف محددة على كل مستوى وفي كل مجال في بنك الإستثمار العربي الأردني لدعم الأهداف الشاملة ومتطلبات أصحاب المصلحة وبذلك يتم المواءمة بين إحتياجات البنك وحلول وخدمات تقنية المعلومات ودعمها بشكل فاعل.

أولاً: دوافع أصحاب المصلحة تؤثر في إحتياجاتهم

تتأثر إحتياجات أصحاب المصلحة بعدد من الدوافع. على سبيل المثال التغييرات الإستراتيجية وتغير بيئة الأعمال والقواعد التنظيمية والتقنيات الجديدة.

ثانياً: إحتياجات أصحاب المصلحة تتبع إلى أهداف المؤسسة

يمكن الربط بين إحتياجات أصحاب المصلحة ومجموعة من الأهداف المؤسسية العامة. تلك الأهداف المؤسسية قد تم تطويرها بإستخدام أبعاد بطاقة الأداء المتوازن BSC وهي تمثل قائمة من الأهداف كثيرة الإستخدام التي قد تضعها المؤسسة لنفسها. على الرغم من أن هذه القائمة ليست حصرية إلا أن معظم الأهداف الخاصة بالمؤسسة يمكن مناظرتها بسهولة لواحد أو أكثر من الأهداف المؤسسية العامة..

ثالثاً: أهداف المؤسسة تتسلسل إلى أهداف التوافق.

يتطلب تحقيق الأهداف المؤسسية عدد من النتائج المتعلقة بأهداف التوافق والتي يعبر عنها بالأهداف المؤسسية المعلوماتية و يتطلب تحقيق الأهداف المؤسسية عدد من النتائج المتعلقة بتقنية المعلومات. والتي يعبر عنها بالأهداف المؤسسية المعلوماتية أو المتعلقة بتقنية المعلومات.

رابعاً: أهداف التوافق تتبع إلى أهداف عناصر التمكين.

يتطلب تحقيق أهداف المواءمة تطبيق عدد من عناصر التمكين وإستخدامها بنجاح. تشمل عناصر التمكين مايلي:

- المبادئ والسياسات وأطر العمل.
- عمليات حاكمية تكنولوجيا المعلومات.
- الهياكل التنظيمية.
- المعلومات والتقارير.
- الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات.
- المعارف والمهارات والخبرات.
- منظومة القيم والأخلاق والسلوكيات

الملحق أ: منظومة السياسات (حد أدنى)

* يستند الجدول أدناه إلى المرفق (6) من تعليمات البنك المركزي الأردني رقم (2016/65) سيعتمد البنك القائمة التالية من الحد الأدنى من السياسات لتنظيم وإدارة العمليات في البنك.

| المنطقة | الغرض | اسم السياسة |
|--|---|--|
| عمليات وخدمات ومشاريع 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. | حاكمية تنظيم تكنولوجيا المعلومات |
| كافة المعلومات والتكنولوجيا المصاحبة لها. | وضع القواعد والمعايير اللازمة لضمان متطلبات الحماية والسرية والمصادقية والتوافرية والامتثال لإدارة موارد تكنولوجيا المعلومات بحسب المعايير الدولية المقبولة بهذا الخصوص مثل ISO-IEC (27001/2) | أمن وحماية المعلومات |
| عمليات البنك الحرجة، وحماية البشر. | 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. | خطط استمرارية العمل وخطط التعافي من الكوارث. |
| كافة عمليات البنك ومدخلاتها الخاصة بتكنولوجيا 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. | إدارة مخاطر تكنولوجيا المعلومات |
| كافة عمليات البنك بمواضيع تكنولوجيا المعلومات. | وضع القواعد والمعايير اللازمة لضمان الامتثال لتعليمات البنك المركزي والجهات الرقابية الأخرى وللقوانين والأنظمة السارية ولسياسات البنك. | الامتثال (IT Compliance) |
| كافة البيانات الخاصة. | وضع القواعد والمعايير اللازمة لحماية البيانات الخاصة المتعلقة بأفراد طبيعيين أو اعتباريين من عمليات الإفصاح والاستخدام غير المصرح به. من عمليات الإفصاح والاستخدام غير المصرح به. | خصوصية البيانات (Data Privacy) |

| النطاق | الغرض | اسم السياسة |
|---|--|--|
| كافة عمليات البنك. | اعتماد سياسة عامة للاستعانة بالموارد بشكل عام وبموارد تكنولوجيا المعلومات بشكل خاص. تلك الموارد سواء المملوكة للبنك (In-sourcing) أو المملوكة للغير (Outsourcing) تراعي التعليمات والأنظمة والقوانين وحاكي أفضل الممارسات الدولية المقبولة بهذا الخصوص. وتأخذ بعين الاعتبار مكان العملية الإنتاجية. (Off-site, Near-site, Off-shore, On-site) وتأخذ بعين الاعتبار وتراعي متطلبات مراقبة مستوى وتفعيل حق تدقيق الخدمات (Service Levels) من قبل أطراف ثالثة محايدة موثوقة (Audit Right). وتحقق متطلبات استمرارية العمل وضوابط الحماية اللازمة لتلبية متطلبات السرية والمصادقية بالإضافة لمتطلبات الكفاءة والفعالية في استغلال الموارد. | التعهد (Outsourcing) |
| كافة مشاريع البنك المتعلقة بتكنولوجيا المعلومات. | وضع القواعد والمعايير اللازمة لإدارة المشاريع بما في ذلك مراحل المشروع وحاكميته اللازمة لتحقيق المتطلبات المتعلقة بالجودة (Quality Requirements) وتلك المتعلقة بالحماية والسرية (Confidentiality Requirements) وتلك المتعلقة بالامتثال تحقيقاً لأهداف البنك وعملياته. | إدارة المشاريع (Project Portfolio Management) |
| البيانات والأجهزة والبرامج والأدوات المصاحبة لها. | وضع القواعد والمعايير اللازمة لتصنيف درجة مخاطر البيانات والأنظمة المختلفة. وتحديد مآلكيه وضوابط حمايتها خلال مراحل دورة حياتها المختلفة. | إدارة الموجودات (Asset Management) |
| الأجهزة والبرمجيات والتطبيقات والشبكات بما في ذلك الإنترنت والبريد الإلكتروني | وضع القواعد والمعايير اللازمة لتحديد السلوك المقبول وغير المقبول لموارد تكنولوجيا المعلومات. | الاستخدام المقبول لموارد تكنولوجيا المعلومات |

| اسم السياسة | الغرض | النطاق |
|--|--|--|
| إدارة التغيير | وضع القواعد والمعايير اللازمة لضمان مصداقية التغيير من حيث توثيق الموافقات اللازمة من مالكي الأصول الخاضعة للتغيير. | كافة عمليات تكنولوجيا المعلومات. |
| أجهزة الكمبيوتر المركزية (Change Management) | ضع 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 والبرمجيات المختلفة بما في ذلك ضوابط الحماية وآليات المراقبة والصيانة الدورية لتلك الأجهزة. | كافة الأجهزة المركزية 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 تلبيةها لمتطلبات العمل من خلال منهجيات التطوير المختلفة المناسبة 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. |

| النطاق | الغرض | اسم السياسة |
|---|--|--|
| البيانات في بيئات التشغيل وحيثما يلزم. | وضع قواعد ومعايير لآليات النسخ الاحتياطي والاسترجاع لضمان توافرية البيانات ومصداقيتها وسريتها. | النسخ الاحتياطي والاسترجاع (Back-up and Restore) |
| كافة الأجهزة والبرمجيات ووسائل وأدوات الاحتفاظ بالبيانات. | وضع القواعد والمعايير الخاصة بحجم البيانات الواجب توأفها سواء بشكل ورقي أو تلك المتواجدة على أجهزة الكمبيوتر (On- Line Data) والتطبيقات المختلفة والمدة الزمنية الواجب الاحتفاظ بها والمفاضلة بين حجم البيانات المتوافرة والسرعة والأداء في الوصول إلى البيانات. | الاحتفاظ بالبيانات (Retention) |
| كافة التجهيزات التقنية والبرامج المتعلقة بها. | وضع قواعد ومعايير للمفاضلة بين المزودين الخارجيين. | شراء الأنظمة والتجهيزات (Purchasing) |
| 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 (Frame relay, ISDN, VPN, DSL, MPLS) | و وضع قواعد ومعايير للربط الشبكي عن بعد بشبكات الكمبيوتر الخاصة بالبنك. لتقليل مخاطر الاطلاع والاستخدام لبيانات ومصادر البنك الحساسة والأنظمة الضبط والرقابة الداخلية المعنية بحماية موجودات البنك. وللحماية من مخاطر السمعة. | النفاز عن بعد (Remote Access) |

| الاسم للسياسة | الغرض | النطاق |
|---|--|---|
| الشبكات (Networks) | وضع قواعد ومعايير لضمان تحقيق متطلبات الكفاءة والفعالية في استغلال عناصر الشبكات والاتصالات من جهة وتحقيق متطلبات الأمن والحماية من جهة أخرى دعماً لتحقيق أهداف البنك. | كافة عناصر الشبكات بكافة البيئات. |
| الشبكات اللاسلكية (Wireless Networks) | وضع قواعد ومعايير بفرض 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 والمعايير الناظمة لتفعيلها (Firewalls) لآلية عمل وحماية أجهزة بالشكل المطلوب الكفيل بحماية وضمان سرية ومصداقية بيانات وعمليات البنك وتوافريتها. | كافة أجهزة ال (Firewalls) 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 بنود أدناه إلى المرفق (7) من تعليمات البنك المركزي الأردني رقم (2016/65) سيستمد 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 مقدمة RACI 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. استراتيجيات 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

تستند البنود أدناه إلى المرفق (8) من تعليمات البنك المركزي الأردني رقم (2016/65)

سيعتمد بنك الإستثمار العربي الأردني 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

الملحق د : التعريفات

المؤسسة:

بنك الإستثمار العربي الاردني.

البنك:

بنك الإستثمار العربي الاردني .

الحاكمية:

تضمن الحاكمية تقييم احتياجات أصحاب المصلحة وشروطهم وخياراتهم من أجل تحديد أهداف متوازنة و متفق عليها على مستوى المؤسسة يتم تحقيقها؛ وتحديد الاتجاه من خلال تحديد الأولويات واتخاذ القرارات؛ ورصد الأداء والامتثال للاتجاه المتفق عليه والأهداف.

كوبت:

تعرف سابقا "بأهداف الرقابة على المعلومات والتكنولوجيا ذات الصلة: كوبت": وتستخدم الآن فقط كإسم في الإصدار الاخير. إطار كامل ومقبول دوليا لحوكمة وإدارة المعلومات والتكنولوجيا المصاحبة لها. يدعم هذا الاطار المدراء التنفيذيين في المؤسسة والإدارة في تعريفها وتحقيق أهداف العمل وأهداف التوافق ذات الصلة. يصف كوبت مبادئ سبع عناصر تمكينية تدعم المؤسسات في تطوير وتنفيذ وتحسين ومراقبة ممارسات الحاكمية والإدارة الجيدة المتعلقة بتكنولوجيا والمعلومات.

التحكم:

وسائل إدارة المخاطر. بما في ذلك السياسات والإجراءات والمبادئ التوجيهية والممارسات أو الهياكل التنظيمية التي يمكن أن تكون ذات طبيعة إدارية أو فنية أو إدارية أو قانونية. وتستخدم أيضا كداعم للحماية أو المضادة.

هدف المؤسسة:

هدف العمل.

إطار الحوكمة:

الإطار هو هيكل أساسي يستخدم لحل أو معالجة القضايا المعقدة؛ وهو عامل تمكين للحكم؛ مجموعة من المفاهيم والافتراضات والممارسات التي تحدد كيف يمكن الاقتراب من شيء ما أو فهمه. والعلاقات بين الكيانات المعنية. وأدوار المعنيين. والحدود (ما هو مدرج وغير المدرج في نظام الحكم).
حوكمة تكنولوجيا المعلومات في المؤسسة:

رؤية للحوكمة تضمن المعلومات ودعم التكنولوجيا ذات الصلة وتمكن من إستراتيجية المؤسسة من تحقيق أهدافها. ويشمل أيضا الحاكمية الوظيفي لتكنولوجيا المعلومات. أي ضمان توفير قدرات تكنولوجيا المعلومات بكفاءة وفعالية.

هدف التوافق:

بيان يصف النتيجة المرجوة من تكنولوجيا والمعلومات في المؤسسة لدعم أهدافها. ويمكن أن تكون النتيجة حرفة أو تغيرا كبيرا في الحالة أو تحسنا كبيرا في القدرات. العملية: عموما. مجموعة من الممارسات التي تتأثر بسياسات الشركة وإجراءاتها التي تأخذ مدخلات من عدد من المصادر (بما في ذلك العمليات الأخرى). تتعالج المدخلات وتنتج المخرجات على سبيل المثال. المنتجات والخدمات.

مجلس الإدارة:

مجلس إدارة البنك.

الإدارة التنفيذية العليا:

تشمل مدير عام البنك أو المدير الإقليمي و نائب المدير العام أو نائب المدير الإقليمي و مساعد المدير العام أو مساعد المدير الإقليمي و المدير المالي و مدير العمليات و مدير إدارة المخاطر و مدير التدقيق الداخلي و مدير الخزانة (الإستثمار) و مدير الإمتثال, بالإضافة لأي موظف في البنك له سلطة تنفيذية موازية لأي من سلطات أي من المذكورين و يرتبط وظيفيا مباشرة بالمدير العام.

أصحاب المصلحة:

أي طرف معني في البنك, مثل المساهمين أو الموظفين أو الدائنين أو العملاء أو الموردين أو الهيئات التنظيمية الخارجية المعنية.

المصادر والمراجع

- أ. تعميم البنك المركزي رقم (2016/65) و تعميم رقم (10-6-984)
- ب. إطار الحوكمة كويت 2019