دليل حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها

مصرف الراجحي - فروع الأردن

This document contains information that is confidential and proprietary to Al-Rajhi Bank. Any dissemination, distribution, copying, use of, or reliance upon all or part of the confidential and proprietary information contained herein is unauthorized and strictly prohibited. All registered trademarks contained herein are the property of their respective holders. Al-Rajhi Bank ©

Template v5.0

المحتويات

1مقدمة..... 3
1-1الغرض من الدليل..... 3
1-2الجهة المسؤولة عن الدليل..... 3
1-3تعديل الدليل..... 3
1-4تعريفات..... 3
2حاكمية و إدارة المعلومات و التكنولوجيا المصاحبة لها..... 5
2-1أهداف حاكمية و إدارة المعلومات و التكنولوجيا المصاحبة لها..... 5
2-2مبادئ الحوكمة..... 6
2-3إطار الحوكمة..... 8
2-4التفاعل بين مجلس الإدارة (ممثلا باللجنة التوجيهية لتكنولوجيا المعلومات) و الإدارة التنفيذية 8
3اللجنة التوجيهية لتكنولوجيا المعلومات (لجنة حاكمة تكنولوجيا المعلومات)..... 8
4حدود المسؤولية..... 10
4-1الإدارة التنفيذية العليا..... 10
4-2الحوكمة..... 10
4-3لجنة التدقيق والمدقق الداخلي و الخارجي..... 11
4-4الاستراتيجية والتخطيط..... 12
5الامن و البنية التحتية لتكنولوجيا المعلومات..... 12
5-1أمن المعلومات..... 12
5-2الأمن المادي..... 12
5-3 البنية التحتية لتكنولوجيا المعلومات..... 13
6 نطاق وآلية تطبيق وتبني نظام حاكمية وادارة المعلومات والتكنولوجيا المصاحبه لها ومهام الأطراف الرئيسيه: 13
7المراجع:..... 14

1 مقدمة

تعتبر موارد تكنولوجيا المعلومات مرتكزا مهما من حيث الحجم النسبي ومن حيث التأثير على قدرة المؤسسة على تسيير عملياتها و بالتالي تحقيق اهدافها، كما و تلعب دورا حساسا في التأثير على تنافسية منتجات و خدمات المؤسسة من جهه و على آليات صنع القرار و ادارة المخاطر من جهه أخرى ، و هذا يبرر حجم الاستثمارات الضخمه في قطاع تكنولوجيا المعلومات من قبل المؤسسات الماليه مما استوجب أن تقوم المؤسسات الماليه باتباع المرتكزات و المعايير السليمة في ادارة موارد تكنولوجيا المعلومات بحسب الممارسات الدوليه المقبوله بهذا الخصوص لتقليل مخاطرها و تجنبا للدخول في استثمارات غير مجديه و مصاريف غير مبرره تترجم الى خسائر طائلة تمتد عبر السنوات و التي قد تنال في بعض الاحيان من سمعة المؤسسة.
ومن منطلق اهتمام المصرف الراجحي-فروع الأردن بتطبيق قواعد ومرتكزات الحوكمة المؤسسية فقد ارتأى إعداد دليل خاص بحاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها، يكمّل دليل الحوكمة المؤسسية وينسجم مع تعليمات البنك المركزي الخاصة بتعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم 2016/65 والصادرة بتاريخ 2016/10/25، وتعميم البنك المركزي رقم 984/6/10 بتاريخ 2019/1/21 الذي اعتمد الاطار المرجعي COBIT 2019 واية تعليمات لاحقة تتعلق بحاكمية تكنولوجيا المعلومات

1-1 *الغرض من الدليل*

تهدف هذه الوثيقة إلى ترسيخ ممارسات حاكمية واضحة و محكمة و فاعلة لادارة المعلومات و التكنولوجيا المصاحبة لها تكون الأساس الذي تقوم عليه ريادة مصرف الراجحي للسوق في المستقبل بما يضمن استمرارية ربحيته و استقراره طويل المدى. كما تؤسس هذه الوثيقة بشكل أخص أعلى المعايير و أفضل الممارسات في حاكمية ادارة المعلومات و التكنولوجيا المصاحبة لها مع تركيز خاص على متطلبات الجهات الرقابية ذات الصلة و أفضل الممارسات العالمية المتبعة في هذا المجال بما ينعكس بشكل إيجابي على جودة منتجات و خدمات المصرف من جانب و على آليات صنع القرار و إدارة المخاطر من جانب آخر.

و يتناول هذا الدليل سجلاً شاملاً و مفصلاً لإطار و آليات حاكمية ادارة المعلومات و التكنولوجيا المصاحبة لها لمصرف الراجحي – فروع الأردن و ذلك استنادا لدليل الحوكمة المؤسسية الخاص بمجموعة الراجحي في المملكة العربية السعودية مع الأخذ بعين الاعتبار متطلبات البنك المركزي الأردني لتوائم سلامة الجهاز المصرفي ككل و إلتزاماً بالمعايير الدولية للممارسات المصرفية السليمة.

2-1 *الجهة المسؤولة عن الدليل*

يكون دليل حاكمية ادارة المعلومات و التكنولوجيا المصاحبة لها في الاردن ضمن مسؤوليات وحدة حاكمية تكنولوجيا المعلومات/دائرة الحوكمة بالاردن و اللجنة التوجيهية لتكنولوجيا المعلومات-مصرف الراجحي الاردن.

و يتولى مدير دائرة الحوكمة إعداد سجل حفظ يتضمن دليل حاكمية ادارة المعلومات و التكنولوجيا المصاحبة لها لمصرف الراجحي فروع الاردن و جميع المستندات و الوثائق ذات الصلة بهذا الدليل.يقوم المصرف بنشر هذا الدليل على موقعه الإلكتروني ليكون متاحا أمام موظفي المصرف و الجمهور.

3-1 *تعديل الدليل*

يكون مدير دائرة الحوكمة مسؤولا عن مراجعة و تحديث محتوى الدليل كلما اقتضت الحاجة وبحيث يتم اعتماده من قبل اللجنة التوجيهية لتكنولوجيا المعلومات وفق تعليمات البنك المركزي الأردني 2016/65 وتعميم البنك المركزي الأردني 984/6/10 بتاريخ 21.1.2019 والتي سمح بها للبنوك الأجنبية بأن تقوم اللجنة التوجيهية لتكنولوجيا المعلومات مقام لجنة حاكمية تكنولوجيا المعلومات (مجلس الإدارة) .

4-1 *تعريفات*

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

حاكمية المعلومات والتكنولوجيا المصاحبة لها : توزيع الأدوار و المسؤوليات و توصيف العلاقات بين الأطراف و الجهات المختلفة و أصحاب المصالح (مثل المجلس ممثلا باللجنة التوجيهية لتكنولوجيا المعلومات و الإدارة التنفيذية) بهدف تعظيم القيمة المضافة للمؤسسة باتباع النهج الأمثل الذي يكفل الموازنه بين المخاطر و العوائد المتوقعة، من خلال اعتماد القواعد و الأسس و الآليات اللازمة لصنع القرار و تحديد التوجهات الاستراتيجية و الأهداف في المصرف وآليات مراقبة و فحص امتثال مدى تحققها بما يكفل ديمومة و تطور المصرف.

الحاكمية المؤسسية : النظام الذي يُوجَه و يدار به المصرف، و الذي يهدف إلى تحديد الأهداف المؤسسية للمصرف و تحقيقها، و إدارة عمليات المصرف بشكل آمن، و حماية مصالح المودعين و أصحاب حسابات الاستثمار، و الالتزام بالمسؤولية الواجبة تجاه المساهمين و أصحاب المصالح الآخرين، و التزام المصرف بالتشريعات و سياسات المصرف الداخلية.

إدارة المعلومات والتكنولوجيا المصاحبة لها: مجموعة النشاطات المستمرة التي تقع ضمن مسؤولية الإدارة التنفيذية و تشمل التخطيط بغرض تحقيق الأهداف الاستراتيجية بما يشمل المواءمة و التنظيم، و نشاطات البناء و التطوير بما يشمل الشراء و التنفيذ، و نشاطات التشغيل بما يشمل توصيل الخدمات و الدعم، و نشاطات المراقبة بما يشمل القياس و التقييم، و بما يكفل ديمومة تحقيق أهداف المصرف و توجهاته الاستراتيجية.

عمليات حاكمية تكنولوجيا المعلومات: مجموعة الممارسات و النشاطات المنبثقة عن سياسات المؤسسة و اللازمة لتحقيق أهداف المعلومات والتكنولوجيا المصاحبة لها.

أهداف المعلومات والتكنولوجيا المصاحبة لها: مجموعة الأهداف الرئيسية و الفرعية المتعلقة بنشاطات الحاكمية و الإدارة للمعلومات و التكنولوجيا المصاحبة لها و اللازمة لتحقيق الأهداف المؤسسية.

أهداف المواءمة: مجموعة الأهداف الرئيسية والفرعية المتعلقة بنشاطات الحاكمية و الإدارة للمعلومات و التكنولوجيا المصاحبة لها و اللازمة لتحقيق الأهداف المؤسسية.

الأهداف المؤسسية: مجموعة الأهداف المتعلقة بالحاكمية و الإدارة المؤسسية و اللازمة لتحقيق احتياجات أصحاب المصالح و أهداف هذه التعليمات.

المجلس: يمثل المجلس اللجنة التوجيهية لتكنولوجيا المعلومات - الأردن.

الإدارة التنفيذية العليا : تشمل المدير الإقليمي أو نائب المدير الإقليمي أو مساعد المدير الإقليمي و المدير المالي و مدير العمليات و مدير إدارة المخاطر و مدير التدقيق الداخلي و مدير الإدارة الشرعية و مدير الخزينة (الاستثمار) و مدير الالتزام و مدير دائرة تكنولوجيا المعلومات، بالإضافة لأي موظف في المصرف له سلطة تنفيذية موازية لأي من سلطات أي من المذكورين و يرتبط وظيفياً مباشرةً بالمدير الاقليمي.

أصحاب المصالح: أي ذي مصلحة في المصرف مثل المودعين أو أصحاب حسابات الاستثمار، أو المساهمين أو الموظفين أو الدائنين أو العملاء أو الجهات الرقابية المعنية.

الملاءمة: توفر متطلبات معينة في أعضاء اللجنة التوجيهية لتكنولوجيا المعلومات إدارة المصرف و إدارته التنفيذية العليا و أعضاء هيئة الرقابة الشرعية للمصرف.

المساهم الرئيسي: الشخص الذي يملك نسبة (5%) أو أكثر من رأسمال المصرف بشكل مباشر أو غير مباشر.

عضو تنفيذي: عضو مجلس الإدارة او من يمثله الذي يشارك بمقابل في إدارة العمل اليومي للمصرف.

المدقق: الشخص (الطبيعي او المعنوي) او الجهة المختصة بفحص عمليات المصرف المرتكزة على تكنولوجيا المعلومات وبما ينسجم مع متطلبات التعليمات بهذا الخصوص والمتفق معه من قبل إدارة المصرف لتحقيق تلك المتطلبات لفترة لا تقل عن 3 سنوات متتالية ولا تزيد عن 6 سنوات متتالية.

2 حاكمية و إدارة المعلومات و التكنولوجيا المصاحبة لها

يفصل هذا الباب توضيح لاهداف حاكمية و إدارة المعلومات و التكنولوجيا المصاحبة لها للمصرف ، و مبادئ و اطار الحاكمية والتفاعل بين اللجنة التوجيهية لتكنولوجيا المعلومات والإدارة التنفيذية لمصرف الراجحي – فروع الأردن.

2-1 *أهداف حاكمية و إدارة المعلومات و التكنولوجيا المصاحبة لها*

تهدف حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها الى ما يلي:

أ. تلبية احتياجات أصحاب المصالح (Stakeholders needs) من خلال تحقيق أهداف المعلومات و التكنولوجيا المصاحبة لها، و بما يضمن:
1. توفير معلومات ذات جودة عالية كمرتكز يدعم آليات صنع القرار في المصرف.
2. إدارة حصيفة لموارد و مشاريع تكنولوجيا المعلومات، تعظم الاستفادة من تلك الموارد و تقلل الهدر منها.
3. توفير بنية تحتية تكنولوجية متميزة و داعمه تمكن المصرف من تحقيق أهدافه.
4. الإرتقاء بعمليات المصرف المختلفة من خلال توظيف منظومة تكنولوجية كفؤة و ذات اعتمادية متميزة.
5. إدارة حصيفة لمخاطر تكنولوجيا المعلومات تكفل الحماية اللازمة لموجودات المصرف.
6. المساعدة في تحقيق الامتثال لمتطلبات القوانين و التشريعات و التعليمات بالإضافة للامتثال لاستراتيجية و سياسات و إجراءات العمل الداخلية.
7. تحسين نظام الضبط و الرقابة الداخلي.
8. تعظيم مستوى الرضا عن تكنولوجيا المعلومات من قبل مستخدميها بتلبية احتياجات العمل بكفاءة و فعالية.
9. إدارة خدمات الأطراف الخارجية الموكل إليها تنفيذ عمليات و مهام و خدمات و منتجات.

ب. تحقيق الشمولية في حاكمية و إدارة المعلومات و التكنولوجيا المصاحبة لها من حيث الأخذ بالاعتبار ليس فقط التكنولوجيا بحد ذاتها و إنما توفير عناصر تمكين (دعامات) سبعة (Components or Enablers 7) تكون مصاحبة و مكملة لخدمات تكنولوجيا المعلومات تتمثل ب:
1. المبادئ و السياسات و أطر العمل.
2. عمليات حاكمية تكنولوجيا المعلومات.
3. الهياكل التنظيمية.
4. المعلومات والتقارير.
5. الخدمات و البرامج و البنية التحتية لتكنولوجيا المعلومات.
6. المعارف و المهارات و الخبرات.
7. منظومة القيم و الأخلاق و السلوكيات.

و ضرورة توفيرها بمواصفات و أبعاد محددة لتحقيق و خدمة متطلبات و أهداف المعلومات و التكنولوجيا المصاحبة لها ليس فقط في عمليات تكنولوجيا المعلومات و حسب، و إنما في كافة عمليات المصرف المرتكزة على المعلومات و التكنولوجيا المصاحبة لها.

ت. تبني ممارسات و قواعد العمل و التنظيم بحسب أفضل المعايير الدولية كنقطة إنطلاق يتم الإرتكاز و البناء عليها في مجالي حاكمية و إدارة عمليات و مشاريع و موارد تكنولوجيا المعلومات.

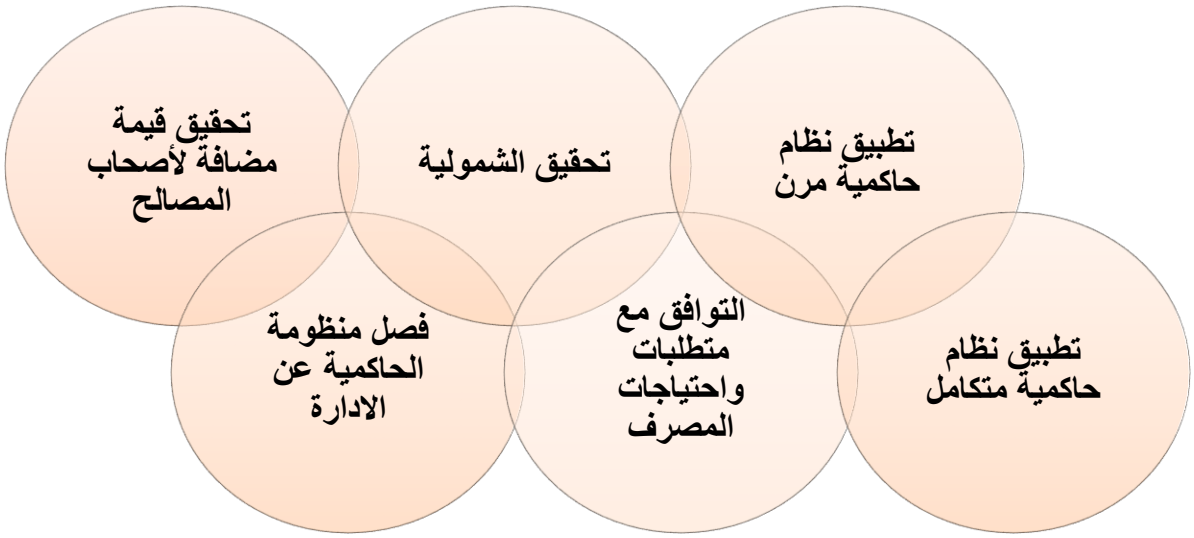
ث. فصل عمليات و مهام و مسؤوليات المجلس أو من يمثله (اللجنة التوجيهية لتكنولوجيا المعلومات) في مجال الحاكمية عن تلك التي تقع ضمن حدود مسؤولية الإدارة التنفيذية بخصوص المعلومات و التكنولوجيا المصاحبة لها.

ج. تعزيز آليات الرقابة الذاتية و الرقابة المســـتقلة و فحص الامتثال في مجالي حاكمية و إدارة المعلومات و التكنولوجيا المصـــاحبة لها و بما يسهم في تحسين و تطوير الأداء بشكل مستمر.

2-2 *مبادئ حاكمية تكنولوجيا المعلومات*

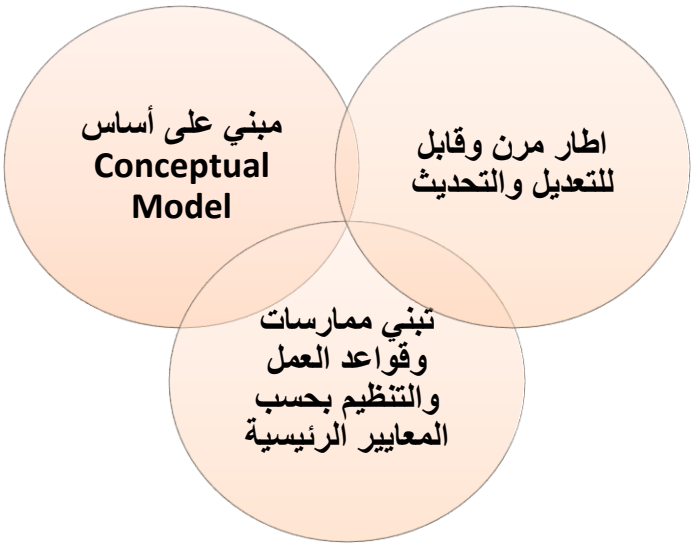
يعتمد إطار الحاكمية لمصرف الراجحي على مجموعتين من المبادئ :
المجموعة الأولى: وهي المبادئ الأساسية والجوهرية التي تشكل نظام الحاكمية Governance System

1- **نطبيق نظام حاكمية مرن**: يجب أن يكون نظام الحاكمية ديناميكيًا ،هذا يعني أنه في كل مرة يكون هناك تغيير في عامل أو أكثر من عوامل التصميم (على سبيل المثال ، تغيير في الاستراتيجية أو التكنولوجيا) ، يجب الأخذ بتأثير هذه التغييرات على نظام الحاكمية.
2- **تحقيق الشمولية:** تم بناء نظام حاكمية تكنولوجيا المعلومات للمؤسسات من عدد من المكونات التي يمكن أن يكون لها أنواع مختلفة و التي تعمل معًا بطريقة شاملة.
3- **تحقيق قيمة مضافة لأصحاب المصلحة**: تحتاج كل مؤسسة إلى نظام حاكمية لتلبية احتياجات أصحاب المصلحة وتوليد قيمة من استخدام تكنولوجيا المعلومات، تعكس القيمة توازنًا بين الفوائد والمخاطر والموارد ، وتحتاج المؤسسات إلى استراتيجية قابلة للتنفيذ و نظام حاكمية تكنولوجيا المعلومات لتحقيق هذه القيمة.
4- **تطبيق نظام حاكمية متكامل**: يجب أن يغطي نظام الحاكمية المؤسسة من البداية إلى النهاية، مع التركيز ليس فقط على وظيفة تكنولوجيا المعلومات ولكن على جميع المعلومات والتكنولوجيا المصاحبة لها التي تضعها المؤسسة لتحقيق أهدافها ، بغض النظر عن مكان معالجة المعلومات في المؤسسة.
5- **التوافق مع متطلبات واحتياجات المصرف**: يجب أن يتم تصميم نظام الحاكمية وفقًا لاحتياجات المؤسسة ، باستخدام مجموعة من عوامل التصميم كمعايير تخصيص وتحديد أولويات مكونات نظام الحاكمية.
6- **فصل منظومة الحاكمية عن الإدارة**: يجب أن يميز نظام الحاكمية بوضوح بين أنشطة وهياكل الحاكمية والإدارة.



المجموعة الثانية: المبادئ المرتبطة باطار الحاكمية Governance Framework اللازمة لبناء نظام الحاكمية على مستوى المصرف.

1- **إطار مرن وقابل للتعديل والتحديث**: يجب أن يكون إطار الحاكمية مفتوحًا ومرنًا كما يسمح بإضافة محتوى جديد والقدرة لمعالجة القضايا الجديدة بأكثر الطرق مرونة، مع الحفاظ على النزاهة والاتساق.
2- **مبني ع أساس Conceptual Model** : يجب أن يقوم إطار الحاكمية على نموذج مفاهيمي، وتحديد المكونات الرئيسية و العلاقات بين المكونات لتحقيق أقصى قدر من الاتساق والسماح بالأتمتة.
3- **تبني ممارسات وقواعد العمل والتنظيم بحسب المعايير الرئيسية**: يجب أن يتماشى إطار الحاكمية مع المعايير والأطر واللوائح الرئيسية ذات الصلة.



3-2 *إطار الحوكمة*

يقوم إطار الحوكمة في مصرف الراجحي - فروع الأردن على مجموعة من لجان الإدارة التنفيذية الداعمة من المستوى الأول و الثاني. و يعتمد هيكل الحوكمة هذا على مجموعة من الركائز الهامة التي تضمن وضوح و انضباط الحوكمة الرشيدة، و هذه الركائز هي: قيم المصرف، تصميم الهيكل التنظيمي، السياسات و الإجراءات، جدول تفويض الصلاحيات و التواصل الفعال بين مختلف الجهات داخل المصرف و كذلك مع الجهات الأخرى خارجه.

4-2 *التفاعل بين مجلس الإدارة (ممثلا باللجنة التوجيهية لتكنولوجيا المعلومات) و الإدارة التنفيذية*

يتولى المجلس و الإدارة التنفيذية العليا توظيف الآليات المختلفة لتشجيع تطبيق السلوكيات المرغوبة و تجنب السلوكيات غير المرغوبة من خلال اتباع أساليب الحوافز و العقوبات على سبيل المثال لا الحصر.

و يراعى لدى انشاء السياسات مساهمة كافة الشركاء الداخليين و الخارجيين و اعتماد أفضل الممارسات الدولية و تحديثاتها كمراجع لصياغة تلك السياسات.

كما يجب مراعاة ضمان فصل المهام المتعارضة بطبيعتها و متطلبات الحماية التنظيمية المتعلقة بالرقابة الثنائية كحد أدنى و كفاية و تحديث الوصف الوظيفي لدى اعتماد و تعديل الهياكل التنظيمية للمصرف.

3 اللجنة التوجيهية لتكنولوجيا المعلومات (لجنة حاكمية تكنولوجيا المعلومات):

تم تشكيل اللجنة التوجيهية لتكنولوجيا المعلومات لتضمن عملية التوافق الاستراتيجي لتكنولوجيا المعلومات لتحقيق الأهداف الاستراتيجية للمصرف بشكل مستدام و التأكد من و متابعة مهام لجنة حاكمية تكنولوجيا المعلومات حيث أنها تقوم بمقامها و تمثلها، و تتكون من " رئيس اللجنة المدير الاقليمي ورئيس مجموعة الدعم نائبا للرئيس و عضوية مدراء الإدارة التنفيذية العليا بما في ذلك مدير تكنولوجيا المعلومات و مدير إدارة المخاطر اضافة الى مدير التدقيق الداخلي كمراقب ، و يمكن لرئيس اللجنه دعوة الغير لدى الحاجة لحضور اجتماعاتها، و توثق اللجنة اجتماعاتها بمحاضر أصولية، على أن تكون دورية الاجتماعات مرة كل ثلاثة أشهر على الأقل، هذا و تتلخص مهام اللجنة فيما يلي:

- ✓ اعتماد الأهداف الاستراتيجية لتكنولوجيا المعلومات و الهياكل التنظيمية المناسبة ، و بما يضمن تحقيق وتلبية الأهداف الاستراتيجية للمصرف وتحقيق أفضل قيمة مضافة من مشاريع و استثمارات موارد تكنولوجيا المعلومات و استخدام الأدوات و المعايير اللازمة لمراقبة و التأكد من مدى تحقق ذلك.
- ✓ اعتماد الإطار العام لإدارة و ضبط و مراقبة موارد و مشاريع تكنولوجيا المعلومات بشكل يحاكي أفضل الممارسات الدولية المقبولة بهذا الخصوص و على وجه التحديد (COBIT).
- ✓ اعتماد مصفوفة الأهداف المؤسسية و أهداف المعلومات و التكنولوجيا المصاحبة لها و توصيف الأهداف الفرعية اللازمة لتحقيقها.
- ✓ اعتماد مصفوفة للمسؤوليات (RACI Chart) تجاه الأهداف الرئيسية لحاكمية تكنولوجيا المعلومات في الاطار المرجعي COBIT 2019 والعمليات الفرعية المنبثقة عنها
- ✓ التأكد من وجود إطار عام لإدارة مخاطر تكنولوجيا المعلومات يتوافق و يتكامل مع الإطار العام الكلي لإدارة المخاطر في المصرف.
- ✓ اعتماد موازنة موارد و مشاريع تكنولوجيا المعلومات بما يتوافق و الأهداف الاستراتيجية للمصرف.
- ✓ الاشراف العام و الاطلاع على سير عمليات و موارد و مشاريع تكنولوجيا المعلومات للتأكد من كفايتها و مساهمتها الفاعلة في تحقيق متطلبات و أعمال المصرف.
- ✓ الإطلاع على تقارير التدقيق لتكنولوجيا المعلومات و اتخاذ ما يلزم من إجراءات لمعالجة الإنحرافات.
- ✓ اعتماد أهمية و ترتيب أولوية أهداف حاكمية و إدارة المعلومات و التكنولوجيا المصاحبة لها و مدى ارتباطها بأهداف المواءمة و الأهداف المؤسسية، بالإضافة لارتباطها بباقي عناصر التمكين (Enablers or Components) السبعة الواردة في التعليمات و ذلك بناء على دراسة نوعية و/أو كمية تعد لهذا الغرض بشكل سنوي على الأقل تأخذ بعين الاعتبار الـ (Design Factors) الواردة في (COBIT 2019 – Design Guide).

- ✓ وضع الخطط السنوية الكفيلة بالوصول للأهداف الاستراتيجية المقرة من قبل المجلس و الإشراف على تنفيذها لضمان تحقيقها و مراقبة العوامل الداخلية و الخارجية المؤثرة عليها بشكل مستمر.
- ✓ ربط مصفوفة الأهداف المؤسسية بمصفوفة أهداف المعلومات و التكنولوجيا المصاحبة لها و اعتمادها و مراجعتها بشكل مستمر و بما يضمن تحقيق الأهداف الاستراتيجية للمصرف و أهداف التعليمات و مراعاة تعريف مجموعة معايير للقياس و مراجعتها و تكليف المعنيين من الإدارة التنفيذية بمراقبتها بشكل مستمر و إطلاع اللجنة على ذلك.
- ✓ التوصية بتخصيص الموارد المالية و غير المالية اللازمة لتحقيق اهداف و عمليات حاكمية تكنولوجيا المعلومات على التوالي و الاستعانة بالعنصر البشري ذو الكفاءة و المناسب في المكان المناسب من خلال هياكل تنظيمية تشمل كافة العمليات اللازمة لدعم الأهداف تراعي فصل المهام و عدم تضارب المصالح و تطويع البنية التحتية التكنولوجية و الخدمات الأخرى المتعلقة بها خدمة للأهداف و تولي عمليات الإشراف على سير تنفيذ مشاريع و عمليات حاكمية تكنولوجيا المعلومات.
- ✓ ترتيب مشاريع و برامج تكنولوجيا المعلومات بحسب الأولوية.
- ✓ مراقبة مستوى الخدمات الفنية و التكنولوجية و العمل على رفع كفاءتها و تحسينها بشكل مستمر.
- ✓ تخصيص الموارد اللازمة و الآليات الكفيلة بتحقيق مهام لجنة حاكمية تكنولوجيا المعلومات.
- ✓ التوصيات باتخاذ الاجراءات المناسبة أي عن أي إنحرافات قد تؤثر سلبا على تحقيق الأهداف الاستراتيجية.
- ✓ مراجعة و بحث أي مخاطر غير مقبولة متعلقة بتكنولوجيا و أمن و حماية المعلومات.
- ✓ تقارير الأداء و الامتثال بمتطلبات الإطار العام لإدارة و ضبط و مراقبة موارد و مشاريع تكنولوجيا المعلومات.
- ✓ تعتبر الأهداف و عمليات حاكمية تكنولوجيا المعلومات و معطياتها حدا أدنى يتوجب على إدارة المصرف العليا الامتثال لها و تحقيقها بشكل مستمر و تعتبر اللجنة التوجيهية لتكنولوجيا المعلومات المسؤول الأول عن ضمان الامتثال بتحقيق متطلباتها (لجنه حاكمية تكنولوجيا المعلومات) ، و يتوجب على كافة دوائر المصرف و على وجه الخصوص دائرة تكنولوجيا المعلومات و إدارة أمن المعلومات و إدارة المشاريع تحديد عملياتها و إعادة صياغتها بحيث تحاكي و تغطي متطلبات كافة عمليات حاكمية تكنولوجيا المعلومات و تشمل المسؤوليات التالية:
  - المسؤولية المباشرة لعمليات التقييم و التوجيه و الرقابة.
  - المسؤولية المباشرة مع دائرة إدارة المخاطر عن عملية "ضمان إدارة حصيفة لمخاطر تكنولوجيا المعلومات" و عملية "إدارة المخاطر".
  - التأكد من اعتماد منظومة المبادئ و السياسات و أطر العمل (Frameworks) اللازمة لتحقيق الإطار العام لإدارة وضبط و مراقبة موارد و مشاريع تكنولوجيا المعلومات وب ما يلبي متطلبات الأهداف و عمليات حاكمية تكنولوجيا المعلومات.
  - التأكد من اعتماد المبادئ و السياسات و أطر العمل و على وجه الخصوص تلك المتعلقة بإدارة مخاطر تكنولوجيا المعلومات و إدارة أمن و حماية المعلومات و إدارة الموارد البشرية و التي تلبي متطلبات عمليات حاكمية تكنولوجيا المعلومات.
  - التأكد من اعتماد السياسات اللازمة لإدارة موارد و عمليات حاكمية تكنولوجيا المعلومات و اعتبار منظومة السياسات هذه حدا أدنى مع إمكانية الجمع و الدمج لتلك السياسات حسب ما تقتضيه طبيعة العمل و على أن يتم تطوير سياسات أخرى ناظمة و مواكبة لتطور أهداف المصرف و آليات العمل على أن تحدد كل سياسة الجهة المالكة و نطاق التطبيق و دورية المراجعة و التحديث و صلاحيات الاطلاع و التوزيع و الأهداف و المسؤوليات و إجراءات العمل المتعلقة بها و العقوبات في حال عدم الامتثال و آليات فحص الامتثال.
  - اعتماد الهياكل التنظيمية (الهرمية و اللجان) و على وجه الخصوص تلك المتعلقة بإدارة موارد و عمليات و مشاريع تكنولوجيا المعلومات و إدارة مخاطر تكنولوجيا المعلومات و إدارة أمن المعلومات و إدارة الموارد البشرية و التي تلبي متطلبات عمليات حاكمية تكنولوجيا المعلومات و تحقيق أهداف المصرف بكفاءة و فعالية.
  - تطوير البنية التحتية و نظم المعلومات اللازمة لتوفير المعلومات و التقارير لمستخدميها كمرتكز لعمليات اتخاذ القرار في المصرف و عليه يجب أن تتوفر متطلبات جودة المعلومات (Information Quality Criteria) و المتمثلة بالمصداقية (Integrity Completeness, Accuracy and Validity) و متطلبات السرية بحسب سياسة تصنيف البيانات و متطلبات التوافرية و الامتثال بتلك المعلومات و التقارير بالإضافة للمتطلبات الأخرى الواردة في المعيار(COBIT 5 – Enabling Information) .

- اعتماد منظومة المعلومات و التقارير و اعتبار تلك المنظومة حدا أدنى، مع مراعاة تحديد مالكي تلك المعلومات و التقارير و تفوض صلاحيات الاطلاع و الاستخدام بحسب الحاجة للعمل و الشركاء المعنيين و يتم مراجعتها و تطويرها بشكل مستمر لمواكبة تطور أهداف و عمليات المصرف و بما يتفق و أفضل الممارسات الدولية المقبولة بهذا الخصوص.
- اعتماد منظومة الخدمات و البرامج و البنية التحتية لتكنولوجيا المعلومات الداعمة و المساعدة لتحقيق عمليات حاكمية تكنولوجيا المعلومات و بالتالي أهداف المعلومات و التكنولوجيا المصاحبة لها وصولاً الى الأهداف المؤسسية.
- منظومة الخدمات و البرامج و البنية التحتية لتكنولوجيا المعلومات و اعتبار تلك المنظومة حداً أدنى و يتم توفيرها و تطويرها بشكل مستمر لمواكبة تطور أهداف و عمليات المصرف و بما يتفق و أفضل الممارسات الدولية المقبولة بهذا الخصوص.
- اعتماد مصفوفة المؤهلات (HR Competencies) و سياسات إدارة الموارد البشرية اللازمة لتحقيق متطلبات عمليات حاكمية تكنولوجيا المعلومات و ضمان وضع الرجل المناسب في المكان المناسب.
- اعتماد منظومة أخلاقية مهنية مؤسسية تعكس القواعد السلوكية المهنية الدولية المقبولة بخصوص التعامل مع المعلومات و التكنولوجيا المصاحبة لها تحدد بوضوح القواعد السلوكية المرغوبة و غير المرغوبة و تبعاتها.
- توظيف الآليات المختلفة لتشجيع تطبيق السلوكيات المرغوبة و تجنب السلوكيات غير المرغوبة من خلال اتباع أساليب الحوافز و العقوبات على سبيل المثال لا الحصر.

4 حدود المسؤولية

4-1 *الإدارة التنفيذية العليا*

تتولى ادارة المصرف التنفيذية لمصرف الراجحي فروع الاردن المسؤوليات التالية:

- ✓ توظيف العنصر البشري المؤهل و المدرب من الأشخاص ذوي الخبرة في مجالات إدارة موارد تكنولوجيا المعلومات و إدارة المخاطر و ادارة أمن المعلومات و إدارة تدقيق تكنولوجيا المعلومات اعتمادا على معايير المعرفة الأكاديمية و المهنية و الخبرة العملية باعتراف جمعيات دولية مؤهلة بموجب معايير الاعتماد الدولي للمؤسسات المانحة للشهادات المهنية (ISO/IEC 17024) و/أو أي معايير أخرى موازية كل بحسب اختصاصه على أن يتم إعادة تأهيل وتدريب الكوادر الموظفة حالياً لتلبية المتطلبات المذكورة خلال سنتين من تاريخ هذه التعليمات.
- ✓ الاستمرار برفد موظفيها ببرامج التدريب و التعليم المستمر للحفاظ على مستوى من المعارف و المهارات يلبي و يحقق عمليات حاكمية تكنولوجيا المعلومات.
- ✓ تتولى الإدارة التنفيذية في المصرف تضمين آليات التقييم السنوي (Performance Evaluation) للكوادر بمعايير قياس موضوعية تأخذ بعين الاعتبار المساهمة من خلال المركز الوظيفي بتحقيق أهداف المصرف.
- ✓ إعداد الاستراتيجيات والسياسات التي تغطي كافة المجالات المتعلقة بتكنولوجيا وامن وحماية المعلومات والمخاطر المصاحبة لها لدى المصرف وتعميمها على المستويات الإدارية المعنية ومراجعتها بانتظام للتأكد من شمولها لأي تعديلات او تغييرات قد تطرأ على القوانين والتعليمات واي امور اخرى تتعلق بالمصرف. وهذا بالإضافة الى اعتماد إجراءات العمل الخاصة بتنفيذ السياسات بشكل يضمن تحديد وقياس وضبط ومراقبة المخاطر المتعلقة بتكنولوجيا المعلومات وبما يلبي متطلبات عمليات حاكمية تكنولوجيا المعلومات.

4-2 *الحوكمة*

تهدف هذه الوثيقة إلى ترسيخ ممارسات حوكمة واضحة ومحكمة وفاعلة لتكون الأساس الذي تقوم عليه ريادة مصرف الراجحي للسوق في المستقبل بما يضمن استمرارية ربحيته واستقراره طويل المدى. كما تؤسس هذه الوثيقة بشكل أخص أعلى المعايير وأفضل الممارسات في حاكمية تكنلوجيا المعلومات مع تركيز خاص على متطلبات الجهات الرقابية ذات الصلة وأفضل الممارسات العالمية المتبعة في مجال حاكمية تكنولوجيا المعلومات.

3-4 *لجنة التدقيق والمدقق الداخلي و الخارجي*

تتولى ادارة التدقيق الداخلي و المدقق الخارجي(مستقل عن إدارة التدقيق الداخلي) لمصرف الراجحي فروع الاردن المسؤوليات التالية:

- ✓ على لجنة التدقيق المنبثقة عن المجلس رصد الموازنات الكافية و تخصيص الأدوات و الموارد اللازمة بما في ذلك العنصر البشري المؤهل من خلال أقسام متخصصة بالتدقيق على تكنولوجيا المعلومات و التأكد من أن كلاً من دائرة التدقيق الداخلي في المصرف و المدقق الخارجي قادرين على مراجعة و تدقيق عمليات توظيف و إدارة موارد و مشاريع تكنولوجيا المعلومات و عمليات المصرف المرتكزة عليها مراجعة فنية متخصصة (IT Audit) من خلال كوادر مهنية مؤهلة و معتمدة دوليا بهذا المجال، حاصلين على شهادات اعتماد مهنية سارية مثل (CISA) من جمعيات دولية مؤهلة بموجب معايير الاعتماد الدولي للمؤسسات المانحة للشهادات المهنية (ISO/IEC 17024) و/أو أي معايير أخرى موازية.
- ✓ تزويد البنك المركزي الأردني بتقرير سنوي للتدقيق الداخلي و آخر للتدقيق الخارجي على التوالي يتضمن رد الإدارة التنفيذية وفق نموذج تقرير تدقيق (مخاطر - ضوابط) المعلومات و التكنولوجيا المصاحبة لها و ذلك خلال الربع الأول من كل عام و تحل هذه التقارير محل نظيرتها أو التي تشملها من التقارير المطلوبة بموجب تعليمات سابقة من البنك المركزي الاردني.
- ✓ تضمين مسؤوليات و صلاحيات و نطاق عمل تدقيق تكنولوجيا المعلومات ضمن ميثاق التدقيق (Audit Charter) من جهة و ضمن إجراءات متفق عليها مع المدقق الخارجي من جهة أخرى و بما يتوافق و يغطي التعليمات.
- ✓ التأكيد للمجلس من قيام المدقق الداخلي و المدقق الخارجي للمصرف لدى تنفيذ عمليات التدقيق المتخصص للمعلومات و التكنولوجيا المصاحبة لها الإلتزام بما يلي:
  - معايير تدقيق تكنولوجيا المعلومات بحسب أخر تحديث للمعيار الدولي) (Information Technology Assurance Framework ITAF الصادر عن جمعية التدقيق والرقابة على نظم المعلومات (ISACA) و منها:
    - تنفيذ مهمات التدقيق ضمن خطة معتمدة بهذا الخصوص تأخذ بعين الاعتبار الأهمية النسبية للعمليات و مستوى المخاطر و درجة التأثير على أهداف و مصالح المصرف.
    - توفير خطط التدريب و التعليم المستمر من قبل الكادر المتخصص بهذا الصدد.
    - الإلتزام بمعايير الاستقلالية المهنية و الإدارية (Independency) Professional and Organizational و ضمان عدم تضارب المصالح الحالية و المستقبلية.
    - الإلتزام بمعايير الموضوعية (Objectivity) و بذل العناية المهنية (Care) Due Professional و الحفاظ المستمر على مستوى التنافسية و المهنية (Proficiency) من المعارف و المهارات الواجب التمتع بها و معرفة عميقة في آليات و عمليات المصرف المختلفة المرتكزة على تكنولوجيا المعلومات و تقارير المراجعة و التدقيق الأخرى (المالية و التشغيلية و القانونية) و القدرة على تقديم الدليل (Evidence)المتناسب مع الحالة و الحس العام في كشف الممارسات غير المقبولة و المخالفة لأحكام القوانين و الأنظمة و التعليمات.
  - فحص و تقييم و مراجعة عمليات توظيف و إدارة موارد تكنولوجيا المعلومات و عمليات المصرف المرتكزة عليها و إعطاء رأي عام (Reasonable Overall Audit Assurance) حيال مستوى المخاطر الكلي للمعلومات و التكنولوجيا المصاحبة لها ضمن برنامج تدقيق يشمل على الأقل المحاور المبينة المطلوبة على 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 الموضح في تعليمات الحاكميه و مرة واحدة كل سنتين على الأقل في حال تم تقييم المخاطر بدرجة (2 أو 1) مع مراعاة التغير المستمر في مستوى المخاطر و الأخذ بعين الإعتبار التغيرات الجوهرية التي تطرأ على بيئة المعلومات و التكنولوجيا المصاحبة لها خلال فترات التدقيق المذكورة، على أن يتم تزويد البنك المركزي الاردني بتقارير التدقيق لأول مرة بغض النظر عن درجة تقييم المخاطر و على أن تشمل عمليات التقييم المحاور المذكورة آليات المصرف المتبعة من حيث التخطيط الاستراتيجي و رسم السياسات و المبادئ و إجراءات العمل المكتوبة و المعتمدة و آليات توظيف الموارد المختلفة بما فيها موارد تكنولوجيا المعلومات و العنصر البشري و آليات و أدوات المراقبة و التحسين و التطوير و العمل على توثيق نتائج التدقيق و تقيمها اعتمادا على أهمية الاختلالات و نقاط الضعف (الملاحظات) بالإضافة للضوابط المفعلة و تقييم مستوى المخاطر المتبقية و المتعلقة بكل منها باستخدام معيار منهجي لتحليل و قياس المخاطر متضمنا الإجراءات التصحيحية المتفق عليها و المنوي اتباعها من قبل

إدارة المصرف بتواريخ محددة للتصحيح مع الإشارة ضمن جدول خاص إلى رتبة صاحب المسؤولية في المصرف مالك كل ملاحظة.

- إجراءات منتظمة لمتابعة نتائج التدقيق للتأكد من معالجة الملاحظات و الاختلالات الواردة في تقارير المدقق بالمواعيد المحددة و العمل على رفع مستوى الأهمية و المخاطر تصعيدا تدريجيا في حال عدم الاستجابة.
- تضمين آليات التقييم السنوي (Performance Evaluation) لكوادر تدقيق تكنولوجيا المعلومات بمعايير قياس موضوعية تأخذ كل ما ورد في البند أعلاه بعين الاعتبار و على أن تتم عمليات التقييم من قبل المجلس ممثلاً بلجنة التدقيق المنبثقة عنه و بحسب التسلسل الإداري التنظيمي لدوائر التدقيق أو من يحل محلها في البنوك الأجنبية.

- من الممكن إسناد(Outsource) دور المدقق الداخلي للمعلومات و التكنولوجيا المصاحبة لها (Internal IT Audit) لجهة خارجية متخصصة مستقلة تماما عن المدقق الخارجي المعتمد بهذا الخصوص شريطة تلبية كافة متطلبات هذه التعليمات و أي تعليمات أخرى ذات صلة و احتفاظ لجنة التدقيق المنبثقة عن المجلس و المجلس نفسه بدورهما فيما يتعلق بفحص الامتثال و التأكد من تلبية هذه المتطلبات كحد أدنى.
- يلتزم المدقق الداخلي و المدقق الخارجي بالامتثال لمنظومة الأخلاق و الممارسات المهنية المعتمدة من قبل المجلس بحيث تتضمن بالحد الأدنى منظومة الأخلاق المهنية الواردة في المعيار الدولي (Information Technology Assurance Framework) الصادر عن جمعية التدقيق والرقابة على نظم المعلومات (ISACA) وتحديثاته.

4-4 *الاستراتيجية والتخطيط*

يدرك مصرف الراجحي أن الإدارة السليمة تعتمد على الرؤية الواضحة و العمليات المحكمة. ومن ثم، يلزم على المصرف أن يضمن تطبيق هذه العمليات و الحرص على اتمامها و أن تتضمن عملية الاستراتيجية و التخطيط ما يلي:

- إعداد و اعتماد مجلس الإدارة لاستراتيجية طويلة المدى (متعددة السنوات) على مستوى المصرف بالكامل توضح الأهداف الاستراتيجية للمصرف عبر المناطق الجغرافية المختلفة و الأسواق المحددة و الأنشطة الداخلية التي يحتاج المصرف لتنفيذها من أجل تحقيق هذه الأهداف.
- توفيق خطط الأعمال و الميزانيات السنوية على مستوى المصرف بالكامل و الإدارات مع الأهداف الاستراتيجية للمصرف مع تحديد الأنشطة و الأهداف السوقية و المالية و التشغيلية و تلك المرتبطة بالعملاء و العائدات المرجحة بالمخاطر.

5 الامن و البنية التحتية لتكنولوجيا المعلومات

1-5 *أمن المعلومات*

تعتبر سرية و تكامل و توفر المعلومات أمراً ضرورياً لحفاظ مصرف الراجحي على ميزته التنافسية و التدفقات النقدية و استمرار ربحيته و الالتزام القانوني و السمعة التجارية. و من هنا، فيلزم على ادارة أمن المعلومات التابعة للمصرف العمل بصفة مستمرة على تحديد و توثيق و تنفيذ و مراجعة إجراءات تأمين نظم المعلومات.

2-5 *الأمن المادي*

يعتبر الأمن المادي للأفراد و الأصول من الجوانب الهامة لعملية إدارة المخاطر داخل مصرف الراجحي و تعمل دائرة الشؤون الإدارية بالمصرف بصفة مستمرة على ضمان اتخاذ الإجراءات المناسبة للتحكم في مخاطر السرقة و الأذى البدني و التي تزيد احتمالات حدوثها بشكل كبير في قطاع المصارف مقارنةً بالصناعات الأخرى و لاسيما نظراً لأن المصارف تتعامل مع كميات كبيرة من المعاملات النقدية.

3-5 *البنية التحتية لتكنولوجيا المعلومات*

يجب مراعاة و توفير التالي في البنية التحتية لتكنولوجيا المعلومات:

- أن تتواجد الغرف و أن يكون تصميم البنية التحتية للبناية بعيدة و محمية عن تهديدات فيضانات و تسربات المياه و الصرف الصحي المحتملة، سواء أسفل البناء أو في نهايته بالقرب من الأسطح أو أي مكان آخر معرض لذلك. كما أن مساحة الغرف يجب أن تكون كافية و تلبي احتياجات المصرف الحالية و تأخذ بالاعتبار التوسع المستقبلي المحتمل.
- يجب أن يكون مكان الغرف و البناية بشكل عام غير محدود الوصول سواء بطبيعة الموقع الجغرافي أو بموجب الاتفاقيات التعاقدية الحصرية من قبل شركات الاتصالات كافة و من مزودين متنوعين.
- يجب أن تتمتع غرف الخوادم الرئيسية وغرف الاتصالات بالحماية المادية و البيئية بحيث تكون محاطة بجدران مسلحة بدون شبابيك و معزولة من حيث التأثيرات الكهرومغناطيسية التي تؤثر سلبا على بيانات أجهزة الكمبيوتر و مخدومة بمدخل احتياطي محكم لاستخدامه من قبل الأفراد عند الطوارئ و يجب أن تكون الغرفة من حيث التصميم مخدومة بمداخل بحسب المواصفات (FM الكهرباء وأجهزة مكافحة الحريق (مثل 200 العالمية و المحلية بهذا الخصوص، كما يجب أن تكون على أرضية (Raised Floor مرفوعة و يجب أن تحتوي على كواشف للدخان و المياه و الحرارة و الرطوبة بدرجة حساسية عالية، كما يجب توفير المراقبة التلفزيونية المسجلة و التبريد الموزع على كافة مساحة الغرفة بشكل عادل لحماية الأجهزة من الحرارة و الرطوبة المرتفعة، مع توفير أجهزة لسحب الغبار، و أن يكون الدخول محكم و مراقب بحيث يمنع غير المخولين من ذلك، مع مراعاة عدم وضع أي إشارات تدل الغير على مكان تواجد تلك الغرف الحساسة في المصرف بدون مرافقين مخولين.
- يجب تزويد غرف الخوادم وغرف الاتصالات بمداخل كهرباء متعددة المصادر و أن يكون التحويل بينها بشكل أوتوماتيكي، أي توفير بطاريات بالإضافة إلى مولدات كهرباء بالقدرة الكافية لتشغيل أجهزة (UPS) و عمليات المصرف (الحساسة على الأقل) في حال انقطاع مصدر الكهرباء الرئيسي.
- يجب الأخذ بالاعتبار متطلبات الدفاع المدني و دائرة المواصفات و المقاييس الأردنية (حيثما تطلب الأمر ذلك).

6 نطاق وآلية تطبيق وتبني نظام حاكمية وادارة المعلومات والتكنولوجيا المصاحبه لها ومهام الأطراف الرئيسيه:

1-6 نطاق وآلية تطبيق وتبني نظام حاكمية وادارة المعلومات والتكنولوجيا المصاحبه لها:

- يشمل نطاق تطبيق التعليمات كافة عمليات المصرف المرتكزة على تكنولوجيا المعلومات بمختلف الفروع والدوائر، وتعتبر جميع الأطراف أصحاب المصالح معنية بتطبيق التعليمات كل بحسب دوره وموقعه.
- تعتبر الاهدف الواردة في الاطار المرجعي COBIT 2019 وباقي عناصر التمكين السبعة المرتبطة بنشاطات تتعلق بمواضيع الامن السيبراني وإدارة المخاطر وخصوصية وحماية البيانات والامتثال والمراقبة والتدقيق والتوافق الاستراتيجي عبارة عن Focus Areas ذات أهمية واولوية عليا.
- يجب ان يتناسب مستوى نضوج (Capability Level) النشاطات المتعلقة بالأهداف الواردة في الإطار المرجعي COBIT 2019 وعناصر التمكين المرتبطة بها بشكل طردي مع درجة الأهمية والاولية بحسب نتائج الدراسة التي تجريها (اللجنة التوجيهية لتكنولوجيا المعلومات) التي تقوم مقام لجنة حاكمية تكنولوجيا المعلومات والمشار اليها أعلاه، على ان لا يقل مستوى النضوج للنشاطات المتعلقة بالاهداف ذات الأهمية والاولوية العليا عن المستوى (3) (Fully Achieved) بحسب سلم النضوج الوارد في الاطار COBIT 2019، ويسمح باعتبار ما لايزيد عن 26% من الأهداف الواردة في الاطار COBIT 2019 ضمن اهداف الإدارة العليا (بما لايزيد عن 9 اهداف بحد اقصى من اصل 35 هدف) على انها اهداف ذات أهمية واولوية ادنى اعتماد على نتائج دراسة نظام حاكمية وادارة المعلومات والتكنولوجيا المصاحبه لها والمعتمده من اللجنة.
- على المصرف عند توقيع اتفاقيات إسناد (Outsourcing) مع الغير لتوفير الموارد البشرية والخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات بهدف تسيير عمليات المصرف التأكد من إلتزام الغير بتطبيق بنود هذه التعليمات بشكل كلي أو جزئي بالقدر الذي يتناسب مع أهمية وطبيعة عمليات المصرف والخدمات والبرامج والبنية التحتية المقدمة قبل وأثناء فترة التعاقد، وبما لا يعفي المجلس والإدارة التنفيذية العليا من المسؤولية النهائية لتحقيق متطلبات التعليمات بما في ذلك متطلبات التدقيق الواردة في الدليل.
- يتوجب على المصرف مواكبة الإصدارات الناشئة المستقبلية وتحديثاتها فيما يخص الإطار العام COBIT وما يحتويه من معايير دولية أخرى مستند لها ضمن هذا الإطار.

- لا بد عند التطبيق والدخول في تفاصيل الدعامات (الممكنات) السبعة والمرفقات والعمليات والأهداف الفرعية أن يقوم المصرف بتطويع (Tailoring) وبما ينسجم ومعطيات المصرف لخدمة أهداف ومتطلبات التعليمات والمعيار COBIT2019 والعمل على إيجاد التغيير المطلوب لتوفير وتهيئة البيئة اللازمة للتطبيق.
- يقوم المصرف باتباع أسلوب تحليل الإنحراف Gap Analysis بين الوضع الحالي والمقارنة مع متطلبات التعليمات والمعيار تمهيدا لعملية التطبيق اخذين بالاعتبار الأهداف التي يسعى المصرف لتحقيقها، الوضع الحالي، الوضع المستقبلي.

2-6 *الأطراف الرئيسيه ومهامها:*

- **رئيس وأعضاء المجلس والخبراء الخارجيين المستعان بهم**: تولي مسؤوليات التوجيه العام لتبني والحفاظ على حاكمية وادارة المعلومات والتكنولوجيا المصاحبه لها بالمستويات المحدده والموافقة على المهام والمسؤوليات، والدعم وتقديم التمويل اللازم.
- **الرئيس التنفيذي ونوابه ومساعديه ورؤساء المجموعات ومسؤولي العمليات ومدراء الفروع**: تولي مسؤوليات تسمية الأشخاص المناسبين من ذوي الخبرة لتمثيلهم في مشاريع وادارة عمليات المعلومات والتكنولوجيا المصاحبه لها وتوصيف مهامهم ومسؤولياتهم.
- **لجنة حاكمية تكنولوجيا المعلومات ممثلة باللجنه التوجيهيه لتكنولوجيا المعلومات**: تولي المسؤوليات المنوطه بموجب المهام الموضحه ضمن البند الثالث من هذا الدليل.
- **التدقيق الداخلي**: تولي مسؤولياته المنوطة به بموجب التعليمات بشكل مباشر، والمشاركة في تبني وتطبيق النظام بما يمثل دور التدقيق الداخلي في الأمور التنفيذية كمستشار ومراقب مستقل.
- **المخاطر والامتثال والقانونية**: تولي مسؤوليات المشاركة في تبني والتأكد من تطبيق مبادىء الحوكمة بما يمثل دور تلك الدوائر.
- **حاكمية تكنولوجيا المعلومات**:
  - الاشراف على مهام واعمال وواجبات عمليات حاكمية انظمة المعلومات والتكنولوجيا المصاحبة لها بما يضمن توافقها مع افضل الممارسات الدوليه في هذا المجال.
  - تقييم تطبيق وتبني كافة عمليات حاكمية انظمة المعلومات والتكنولوجيا المصاحبة لها والمعتمده ضمن نظام الحاكميه المخصص للمصرف والاشراف على وصول وابقاء هذه العمليات ضمن مستويات النضوج المطلوبه بالاعتماد على اتباع أسلوب تحليل الإنحراف Gap Analysis بين الوضع الحالي ونظام حاكمية وادارة المعلومات والتكنولوجيا المصاحبه لها المعتمد، تحقيقا لاهداف واستراتيجيات المصرف.
  - توجيه ومراقبة الامتثال لتعليمات البنك المركزي الأردني بهذا الخصوص.
  - بناء نظام يضمن متابعة ومراقبة مصفوفة الاهداف المؤسسيه الخاصه بالمصرف والية ربطها بمصفوفة اهداف المواءمة، واعتمادها ومراجعة هذه الآليه سنوياً وبشكل مستمر مما يضمن تحقيق الأهداف الاستراتيجية للمصرف.
  - تصميم وبناء نظام حاكمية مخصص لتلبية احتياجات ومتطلبات المصرف بناء على دراسة نوعية و/اوكمية تعد لهذا الغرض وتراجع بشكل سنوي على الأقل وتأخذ بالاعتبار محددات التصميم (Design Factors) والأهداف ذات الأولوية والاهمية العليا (Focus Area)، وضمان مواءمتها مع اهداف واستراتيجية المصرف.
  - مراقبة وتحليل أداء عمليات انظمة المعلومات والتكنولوجيا المصاحبة لها عن طريق مؤشرات الاداء.
  - رفع المواد والتقارير المناسبه لاجتماعات اللجنة ، وضمان شفافية وجودة المعلومات مما يدعم اتخاذ القرارات والتوصيات المناسبه لتحقيق الفائدة، وتعظيم القيمة المضافة لاصحاب المصلحه، ومتابعة إنجاز التكليفات المنبثقة عن هذه اللجان.
  - تولي دور المرشد لنشر المعرفة بالمعيار وتسهيل عملية التطبيق والتبني على ان يتم الاستعانه بالمتخصصين وحملة الشهادات الفنيه والمهنيه الخاصه بالمعيارCOBIT Foundation, COBIT Assessor, COBIT Implementation, CGEIT من داخل المصرف ومن خارجه عند الحاجه.

7 المراجع:

1. تعليمات حاكمية وإدارة المعلومات والتكنولوجيا المصاحبة لها رقم 2016/65 بتاريخ 2016/10/25 الصادرة عن البنك المركزي وتعميم البنك المركزي رقم 948/6/10 بتاريخ 2019/1/21 والمستند على الاطار المرجعي COBIT 2019 والمنشور على موقع البنك المركزي http://www.cbj.gov.jo
2. تعليمات COBIT والصادرة من جمعية التدقيق والرقابة على نظم المعلومات في الولايات المتحدة الأمريكية Information Systems Audit and Control Association (ISACA) والمنشور على موقع الجمعية https://www.isaca.org/COBIT/Pages/Product-Family.aspx

- COBIT 5 Framework
- COBIT 5 Implementation
- COBIT 5 Enabling Process
- COBIT 5 Enabling Information
- COBIT 2019 Framework: Introduction and Methodology
- COBIT 2019 Framework: Governance and Management Objectives
- COBIT 2019 Design Guide: Designing and Information and Technology Governance Solution
- COBIT 2019 Implementation Guide: Implementing and Optimizing and Information and Technology Governance Solution