مصرف أربيل للأستثمار و التمويل
بانكى اربيل بۆ وەبەرهێنان و پێدان
ERBIL BANK FOR INVESTMENT & FINANCE

دليل حوكمة تقنية المعلومات
لمصرف اربيل للاستثمار والتمويل

المحتويات

المصطلحات

المصرف	مصرف أربيل.
المجلس	مجلس إدارة مصرف أربيل.
أعضاء المجلس	أعضاء مجلس إدارة مصرف اربيل سواء بصفتهم الشخصية أو ما ينوب عنهم (بما فيهم رئيس ونائب رئيس المجلس).
حوكمة تقنية المعلومات	توزيع الأدوار والمسؤوليات بين الاطراف والجهات المختلفة وأصحاب المصلحة (مثل المجلس والادارة التنفيذية) باتباع النهج الأمثل الذي يكفل الموازنة بين المخاطر والعوائد المتوقعة، من خلال اعتماد القواعد والاسس والآليات اللازمة لصنع القرار وتحديد التوجهات الاستراتيجية والأهداف في المصرف وآليات مراقبة وفحص امتثال مدى تحققها بما يكفل ديمومة وتطور المصرف.
COBIT	إطار عمل حوكمة تقنية المعلومات تم انشاءه من قبل جمعية المدققين التقنيين الامريكية.
ISACA	جمعية المدققين التقنيين الامريكية.
عمليات حوكمة تقنية المعلومات	مجموعة الممارسات والنشاطات المنبثقة عن سياسات المصرف واللازمة لتحقيق اهداف المعلومات والتقنية المصاحبة لها.
الادارة التنفيذية العليا	تشمل المدير المفوض للمصرف ومدير العمليات ومعاون المدير المفوض ومدير ادارة المخاطر ومدير الامتثال بالإضافة لأي موظف في المصرف له سلطة تنفيذية ويرتبط وظيفياً مباشر ةً بالمدير المفوض.
اصحاب المصلحة	من لديهم مصلحة في المصرف مثل المساهمين أو الموظفين أو العملاء أو المزودين الخارجيين أو الجهات الرقابية المعنية.
Objectives	العمليات الخاصة بتنفيذ نظام الحوكمة بما يتماشى مع سياسة المصرف لتحقيق الاهداف المرجوة
CMMI	مقياس مستوى النضوج المتكامل هو إطار عمل خاص بمراجعة العمليات التقنية وتقييمها وهو المعتمد في قياس ومراجعة العمليات ضمن نظام حوكمة تقنية المعلومات
عوامل التصميم	وهي العوامل المعتمدة في إطار عمل كوبت لتصميم نظام حوكمة تقنية المعلومات المخصصة لاي مؤسسة.
مكونات الاهداف Objective) (Components	المكونات هي عوامل تساهم، بشكل جماعي، في انجاح العمليات الخاصة بنظام الحوكمة لتقنية المعلومات في المؤسسة.

١- المقدمة

أ- نظرة عامة:

مع التطور الحاصل في تقنية المعلومات و اعتماد الاعمال و من ضمنها القطاعات المالية على التقنية الناشئة و ما احدثه توافر تقنية المعلومات و تطوره ظهرت الحاجة الى رفع مستوى الاداء باستخدام تقنية المعلومات و التقنية المصاحبة على مستوى المؤسسات العاملة في مختلف المجالات و ذلك باتباع افضل السبل العلمية و المعايير الدولية و الاطر العالمية في ادارة تقنية المعلومات، و من هذا المنطلق وجهت الادارة العليا في المصرف و المتمثلة برئيس مجلس الادارة و اعضاء مجلس الادارة و تماشيا مع توجهات البنك المركزي العراقي بالشروع بتطبيق اطار عمل كوبت (COBIT) لكافة الاصدارات الحالية و القادمة لتحقيق اعلى قيمة من خلال الموائمة الصحيحة للأعمال والتقنية المصاحبة لها و الحفاظ على رصانة الاعمال المصرفية في العراق كون المصرف جزء من منظومة العمل المصرفي بالعراق.

ب- نبذة عن المصرف:

يعتبر مصرف (اربيل للاستثمار والتمويل) من المصارف الرائدة بالعراق تأسس في عام ٢٠١٠ ولديه اربعة فروع في العراق ويقدم منتجات وخدمات مالية شاملة بما في ذلك الخدمات المصرفية للشركات والأفراد برأس مال وقدره (٢٦٥) مليار دينار عراقي.

ج- الوصف العام:

تشكل هذه الوثيقة دليل عمل إدارة تقنية المعلومات والتقنية المصاحبة في المصرف. باختصار، يعطي لمحة عامة عن السياسات وقواعد الممارسة والمبادئ التوجيهية التي تنطبق على حوكمة تقنية المعلومات في المصرف، كما يوضح التزام المصرف بتوفير التدريب على إدارة تقنية المعلومات والتقنية المصاحبة وزيادة الوعي في هذا المجال.

يجمع هذا الدليل جميع متطلبات حوكمة تقنية المعلومات بحيث تتم معالجة جميع العمليات للتقنية والتقنية المصاحبة بشكل قانوني وآمن وفعال. تلعب تقنية المعلومات دورًا رئيسيًا في العمليات اليومية للمصرف. حيث تعتمد جودة الخدمات والتخطيط وقياس الأداء والضمان والإدارة المالية على المعلومات الدقيقة والمتاحة. تتطلب إدارة تقنية المعلومات القوية هياكل إدارة ومساءلة واضحة وفعالة، وعمليات حوكمة، وسياسات وإجراءات موثقة، وموظفين مدربين وموارد كافية. وفقًا لذلك، يحدد هذا الدليل المتطلبات والمعايير وأفضل الممارسات التي تنطبق على عمليات تقنية المعلومات.

٢- النطاق

أ- يغطي نطاق تطبيق الضوابط كافة عمليات المصرف المرتكزة على تقنية المعلومات والاتصالات بمختلف الفروع والادارات، وتعد جميع الأطراف معنية بتطبيق الضوابط كلا بحسب وظيفته وموقعه، مع الالتزام بالفترات الزمنية المحددة من قبل البنك المركزي العراقي الممتدة لخمس سنوات لإتمام عملية تطبيق حوكمة تقنية المعلومات ويشتمل على:

- جميع الاجهزة والبرامج والادوات والبيانات الإلكترونية المخزنة والمعالجة بواسطة أجهزة الكمبيوتر وأجهزة التخزين الثابتة والمحمولة.
- البيانات المنقولة عبر الشبكات.
- المعلومات المرسلة عن طريق الفاكس او البريد أواي طرق نقل مماثلة.
- جميع العقود والسجلات الورقية والتقارير والسياسات والاجراءات الخاصة بتقنية المعلومات والتقنية المصاحبة.

ب - يمتثل لحوكمة تقنية المعلومات كل من:

- جميع الموظفين العاملين في المصرف.
- الجهات الخارجية المصرح لها بالتعامل مع المصرف فيما يخص تقنية المعلومات والتقنية المصاحبة بما في ذلك على سبيل المثال الاستشاريين ومقدمي الخدمات والمقاولين والزوار.

٣- الادوار والمسؤوليات

ادناه الأطراف المعنية ومسؤولياتها الرئيسية بهذا الشأن:

أ- رئيس واعضاء المجلس والخبراء الخارجيين المستعان بهم: تولي مسؤوليات التوجيه العام والموافقة على المهام والمسؤوليات، والدعم وتقديم التمويل اللازم.

ب- المدير المفوض ومعاونه ومديرو العمليات والفروع: تولي مسؤوليات تسمية الأشخاص المناسبين من ذوي الخبرة بعمليات المصرف وتوصيف مهامهم ومسؤولياتهم.

ج- مدير ولجان تقنية المعلومات والاتصالات التوجيهية ومديرو المشاريع: تولي مسؤوليات الإدارة والتوجيه والإشراف بشكل مباشر، والتوصية بتوفير الموارد اللازمة، والتأكد من الفهم الصحيح من قبل الأطراف كافة بمتطلبات وأهداف الضوابط المحددة في هذا الدليل.

د- التدقيق الداخلي: تولي مسؤولياته المناطة به بموجب هذه الضوابط بشكل مباشر والتوصية بتوفير المعلومات اللازمة لإتمامه، والتأكد من الفهم الصحيح من قبل الأطراف كافة بمتطلبات وأهداف الضوابط المحددة في هذا الدليل.

ه- إدارة المخاطر، وأمن المعلومات، والامتثال، والقانونية: تولي مسؤوليات المشاركة بما يمثل دور تلك الإدارات.

٤- اهداف حوكمة تقنية المعلومات

ان الغرض الرئيسي من تطبيق حوكمة تقنية المعلومات هو انشاء القيمة من خلال الموائمة الحقيقية والفعالة واشراك اصحاب المصلحة الرئيسيين ودعم مجلس الادارة من خلال توجيهاته بتحقيق أهداف المصرف من خلال تحقيق أهداف تقنية المعلومات والاتصالات مع تخصيص كافة الموارد لإنجاح وتحقيق اهداف المصرف.

الاهداف المرجوة من تطبيق حوكمة تقنية المعلومات:

أ- معالجة مخاطر الأعمال المرتبطة بالاستخدام والملكية والتشغيل والمشاركة واعتماد تقنية المعلومات والاتصالات داخل المصرف وتحسين ادارة مخاطر الأعمال المتعلقة بتقنية المعلومات وتأمين الحماية اللازمة لأصول المصرف والحفاظ على القيمة.

ب- تقديم خدمات وحلول مناسبة في الوقت المحدد وضمن الميزانية التي تولد المنافع المالية وغير المالية المقصودة.

ج- قياس قيمة تقنية المعلومات بطريقة تُظهر تأثير ومساهمات الاستثمارات التي تدعم تقنية المعلومات

د- تحسين الموارد وتوفير بنية تحتية متكاملة واقتصادية وداعمة لتقنية المعلومات تمكن المصرف من تحقيق أهدافها

ه- تخفيض تكاليف استمرارية الاعمال المتعلقة بتقنية المعلومات.

و- زيادة القدرة على الابتكار المدعومة بتقنية المعلومات وتوفير معلومات ذات جودة عالية تكون مرتكزا يدعم آليات صنع القرار في المصرف.

ز- زيادة المواءمة بين الاستثمارات الرقمية وأهداف واستراتيجية العمل.

ح- زيادة الثقة بين الأعمال وتقنية المعلومات.

ط- إدارة رشيدة لموارد ومشاريع تقنية المعلومات والاتصالات للإفادة من تلك الموارد، وتقليل الهدر فيها.

ي- الارتقاء بعمليات المصرف المختلفة من خلال توظيف منظومة تقنية كفوءة وذات اعتمادية متميزة.

ك- المساعدة في تحقيق الامتثال لمتطلبات القوانين والتشريعات والضوابط، فضلا عن الامتثال لاستراتيجية وسياسات وإجراءات العمل الداخلية وتحسين نظام الرقابة الداخلي.

ل- تحسين مستوى الرضا عن تقنية المعلومات والاتصالات من قبل مستخدميها بتلبية احتياجات العمل بكفاءة وفعالية.

م- إدارة خدمات الأطراف الخارجية الموكل إليها تنفيذ عمليات ومهام الخدمات والمنتجات المتعلقة بتقنية المعلومات والاتصالات.

٥- السياسات العامة

أ- يستند هذا الدليل على تعليمات البنك المركزي العراقي الصادرة بكتاب البنك المركزي العراقي المرقم ٦١١\١٤ لسنة ٢٠١٩ والمصادر العلمية لإطار عمل كوبت (COBIT Framework) من جمعية المدققين التقنيين الامريكية ISACA.

ب- يتم مراجعة وتحديث هذا الدليل بشكل منتظم من خلال لجنة الحوكمة في المصرف بما يتوائم مع التحديثات الخاصة باللوائح والقوانين الصادرة من البنك المركزي العراقي والاصدارات اللاحقة من المعايير الدولية والاطر العالمية وتحديثات إطار عمل كوبت.

ج- يقوم المصرف بنشر هذا الدليل على الموقع الالكتروني للمصرف واعتماده كمنهجية عمل لإدارة التقنية والتقنية المصاحبة للمصرف.

د- يعتبر هذا الدليل جزء من دليل الحوكمة المؤسسية للمصرف.

٦- اللجان

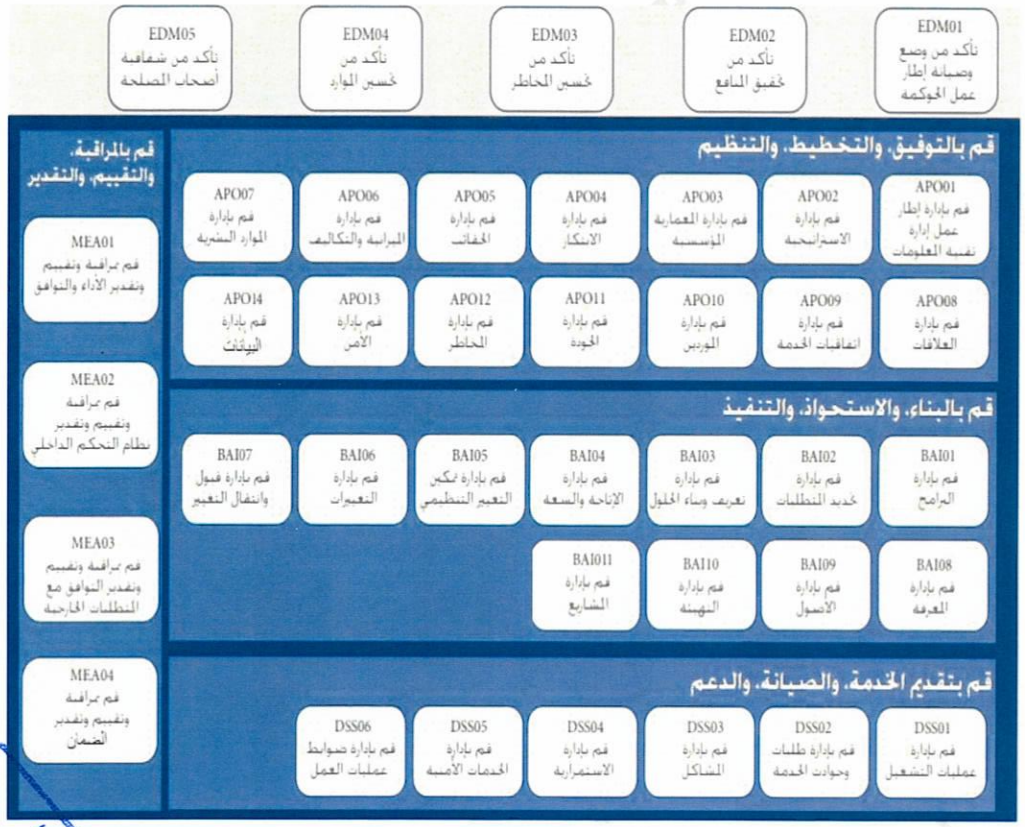
تم تشكيل اللجان المعنية والموضحة ادناه وتعيين مسؤولياتها وادوارها وكما وردت في كتاب البنك المركزي العراقي وتوضيح المهام والادوار الخاصة بها في مواثيقها.

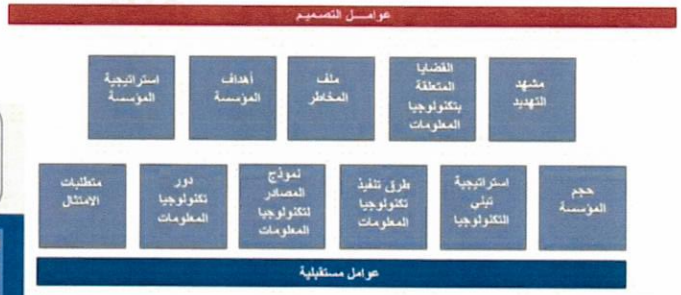
أ- لجنة حوكمة تقنية المعلومات والاتصالات: تتشكل هذه اللجنة من ثلاثة أعضاء مجلس ادارة وتضم في عضويتها أشخاصا من ذوي الخبرة أو المعرفة الاستراتيجية في تقنية المعلومات والاتصالات وتوثق اللجنة اجتماعاتها بمحاضر أصولية، وتجتمع اللجنة دوريا مرة كل ربع سنوي في الأقل.

ب- اللجنة التوجيهية لتقنية المعلومات والاتصالات : تتشكل هذه اللجنة ،برئاسة المدير المفوض والمديرين الفرعيين ، بما في ذلك مدير تقنية المعلومات والاتصالات ومدير إدارة المخاطر ومدير أمن المعلومات ، وينتخب المجلس أحد أعضائه ليكون عضوا مراقبا في هذه اللجنة ، فضلا عن مدير التدقيق الداخلي الذي تكون مهمته مراقبا ، وليس عضوا في اللجنة ، ويتم حضوره فقط حين تقديم أو مناقشة تقريره لتحقيق مبدأ الاستقلالية والموضوعية ، ويمكنها دعوة الغير لدى الحاجة لحضور اجتماعاتها ، وتوثق اللجنة اجتماعاتها بمحاضر أصولية ، وتجتمع اللجنة التوجيهية دوريا مرة كل ربع سنوي في الأقل.

٧- اهداف تقنية المعلومات والتقنية المصاحبة (Objectives) الخاصة بالمصرف

هو نظام حوكمة مصمم خصيصا للمصرف اعتمادا على استراتيجيات واهداف المصرف مع وصف كامل للمخاطر والمشاكل الخاصة باستخدام التقنية والتقنية المصاحبة فهو نظام او مجموعة من العمليات تم اختيارها بناء على ما يحتاجه المصرف وعلى ما يريد ان يحققه من استخدام التقنية والتقنية المصاحبة كما موضحة بالشكل ادناه. والذي يتم انشائه وفقا لمعطيات عوامل التصميم والامتثال لمتطلبات البنك المركزي العراقي، مع الاخذ بنظر الاعتبار إن نظام الحوكمة ديناميكي بطبيعته. يمكن أن تتغير الإستراتيجيات، ويتم إطلاق برامج استثمارية مهمة، وتطور طبيعة التهديدات، وتغيير التقنيات، وما إلى ذلك. وهذا يعني أنه يجب مراجعة نظام الحوكمة على أساس منتظم، ويجب إجراء التغييرات على النظام كلما لزم الأمر.





عوامل التصميم

مناطق التركيز

أهداف المؤسسة المصممة خصيصًا للمعلومات والتكنولوجيا

العمليات الموصى بها من قبل البنك المركزي العراقي (24)

أ- تم اعتماد الاهداف (Objectives) الخاصة بحوكمة تقنية المعلومات للمصرف الموضحة بالمرفق (٢) بما يوائم اهداف المصرف.

ب- يتم اعتماد اهمية و ترتيب الاولوية في الاهداف (Objectives) استنادا الى اهداف المصرف و استراتيجيتها بالاعتماد على المنهجية الموصى بها بتحديد الاهداف الخاصة بالمصرف عن طريق الاعتماد على عوامل التصميم الاحد عشر الخاصة بالمصرف و المتمثلة بـ (إستراتيجية المؤسسة, أهداف المؤسسة , ملف المخاطر , القضايا المتعلقة بـالتقنية المصاحبة , بيئة التهديد ,متطلبات الامتثال , دور تقنية المعلومات , نموذج المصادر لتقنية المعلومات, طرق تنفيذ تقنية المعلومات , استراتيجية تبني التقنية ,حجم المؤسسة) و كما موضحة بالمرفق (١).

ج- يتم اعتماد مقياس (CMMI) في عملية قياس مستوى نضوج العمليات الخاصة بالأهداف (Objectives) الخاصة بالمصرف.

د- يتم تنفيذ الاهداف الخاصة بالمصرف لكافة المكونات السبعة لكل هدف من اهداف المصرف.

٨- مكونات الاهداف (Objective Components)

يتم اعتماد المكونات الخاصة بحوكمة تقنية المعلومات استنادا الى إطار عمل كوبت (COBIT ٢٠١٩) والتي تشتمل على سبع مكونات خاصة بالأهداف (Objectives) لتحقيق نهج شمولي لكافة العمليات الخاصة بإدارة التقنية والتقنية المصاحبة بالمصرف.

أ- **العمليات:** يتم انجاز العمليات الخاصة بكل الاهداف الخاصة بالمصرف على اساس الاعتماد على المراجع والمعايير الموصى بها واتمام عملية مراقبته وقياسها استنادا الى مقياس مستوى النضوج المتكامل (CMMI)

ب- **الهياكل التنظيمية:** يتم تحديد المسؤوليات لكافة العمليات بصورة واضحة واسناد المهام الى الاشخاص والوظائف والاقسام المعنية لإتمام عمل كافة العمليات الخاصة بالمصرف

ج- **السياسات والاجراءات:** يعتمد مجلس إدارة المصرف ولجانه المختصة منظومة السياسات اللازمة لإدارة وتشغيل حوكمة تقنية المعلومات وكما مبينة بالمرفق (٣).

د- **المعلومات:** يتولى مجلس إدارة المصرف والإدارة التنفيذية العليا مسؤولية التأكد من تطوير البنية التحتية والأنظمة اللازمة لتوفير المعلومات والتقارير لأصحاب المصلحة بهدف المساهمة في اتخاذ القرار السليم في المصرف. يعتمد المصرف نظم المعلومات والتقارير المذكورة في

المرفق (٤) حيث تتم مراجعة المعلومات والتقارير وتحديثها لتعكس أهداف الحوكمة والإدارة وفقًا لأفضل الممارسات والمعايير.

ه- **الخدمات والبرامج والبنى التحتية لتقنية المعلومات:** على مجلس الادارة والادارة التنفيذية دعم كافة المبادرات الخاصة بالبرامج والخدمات والبنية التحتية وادامتها.

و- **المعرفة والمهارات والخبرات:** على ادارة المصرف تبني واعتماد مصفوفة المهارات والكفاءات وأفضل المعايير لإدارة الموارد البشرية وزيادة الخبرات والكفاءات بنهج التعليم المستمر لمواكبة التطور الحاصل في تقنية المعلومات والتقنية المصاحبة.

ز- **الثقافة والاخلاقيات والسلوك:** يلتزم مجلس الادارة مع الادارة التنفيذية بنشر وعي الالتزام بالقوانين والاخلاق المهنية بالتعامل مع المعلومات التقنية والتقنية المصاحبة لها مع الاحترافية في العمل وضمان سرية المعلومات.

٩- مبادئ حوكمة تقنية المعلومات

يتم اعتماد المبادئ الخاصة بحوكمة تقنية المعلومات استنادا الى المبادئ الرئيسية لإطار عمل كوبت (COBIT ٢٠١٩) والتي تشتمل على المبادئ الاتية: -

أ- مبادئ نظام الحوكمة

- تلبية احتياجات أصحاب المصلحة لإنشاء القيمة من استخدام تقنية المعلومات والاتصالات حيث تعكس القيمة توازناً بين الفوائد والمخاطر والموارد
- شمولية تطبيق نظام الحوكمة لكل مكونات النظام السبعة الوارد ذكرها في الفقرة الثامنة
- يجب أن يكون نظام الحوكمة ديناميكيًا. هذا يعني أنه في كل مرة يتم تغيير واحد أو أكثر من عوامل التصميم (على سبيل المثال، تغيير في الاستراتيجية أو التقنية)، يجب مراعاة تأثير هذه التغييرات على نظام حوكمة تقنية المعلومات والتقنية المصاحبة.
- الفصل بين مسؤوليات مجلس الادارة والادارة التنفيذية من خلال توزيع الادوار بشكل واضح على كافة المستويات.
- تصميم نظام الحوكمة وفقًا لاحتياجات المصرف، باستخدام عوامل التصميم كمعايير لتخصيص مكونات نظام الحوكمة وترتيبها حسب الأولوية.
- يجب أن يغطي نظام حوكمة تقنية المعلومات المصرف من البداية إلى النهاية بشكل كامل.

ب- مبادئ إطار الحوكمة

- تحديد المكونات الرئيسية والعلاقات بين المكونات، لتحقيق أقصى قدر من الاتساق والسماح بالأتمتة.
- يجب أن يكون إطار الحوكمة مفتوحًا ومرنًا بحيث يسمح بإضافة محتوى جديد والقدرة على معالجة القضايا الجديدة بأكثر الطرق مرونة، مع الحفاظ على النزاهة والاتساق.
- يجب أن يتماشى إطار الحوكمة مع المعايير والأطر واللوائح الرئيسية ذات الصلة.
-

١٠- التدقيق والرقابة الداخلية

على المجلس رصد الموازنات الكافية وتخصيص الأدوات والموارد اللازمة بما في ذلك العنصر البشري المؤهل من خلال فريق متخصص بالتدقيق على تكنولوجيا المعلومات، والتأكد من أن كل من قسم التدقيق الداخلي في المصرف والمدقق الخارجي قادرين على مراجعة وتدقيق عمليات توظيف وإدارة موارد ومشاريع تكنولوجيا المعلومات وعمليات البنك المرتكزة عليها مراجعة فنية متخصصة من خلال كوادر مهنية مؤهلة ومعتمدة دوليا بهذا المجال، حاصلين على شهادات اعتماد مهنية و تزويد البنك المركزي العراقي بتقرير سنوي للتدقيق الداخلي و آخر للتدقيق الخارجي على التوالي يتضمن رد الإدارة التنفيذية و اطلاع وتوصيات المجلس بخصوصه.

المصادر:

١- كتاب البنك المركزي العراقي المرقم ٦١١\١٤ لسنة ٢٠١٩
٢- COBIT® ٢٠١٩ Framework: Introduction and Methodology
٣- COBIT® ٢٠١٩ Design Guide: Designing an Information and Technology

مرفق رقم (١) (عوامل التصميم)

عامل التصميم	وصف عامل التصميم
إستراتيجية المؤسسة	يمكن أن يكون للمؤسسات إستراتيجيات مختلفة، والتي يمكن التعبير عنها على أنها واحدة أو أكثر من النماذج الأصلية للمؤسسات، عادةً استراتيجية أولية واستراتيجية ثانوية واحدة.
أهداف المؤسسة	أهداف المؤسسة التي تدعم إستراتيجية المؤسسة، تتحقق إستراتيجية المؤسسة من خلال تحقيق مجموعة أهداف المؤسسة. تم تحديد هذه الأهداف في إطار COBIT، وهي منظمة وفقًا لأبعاد بطاقة الأداء المتوازن (BSC)، وتشتمل على ثلاث عشر هدف.
ف المخاطر	يحدد ملف تعريف المخاطر نوع المخاطر المتعلقة بتقنية المعلومات التي تتعرض لها المؤسسة حاليًا ويشير إلى مجالات المخاطر التي تتجاوز قابلية المخاطرة.
القضايا المتعلقة بـالتقنية المصاحبة	تمثل إحدى الطرق لتقييم مخاطر التقنية المصاحبة للمؤسسة في النظر في القضايا ذات الصلة بـالتقنية المصاحبة التي تواجهها المؤسسة حاليًا.
بيئة التهديد	وصف لبيئة التهديد الذي تعمل المؤسسة تحته.
متطلبات الامتثال	متطلبات الامتثال التي تخضع لها المؤسسة.
دور تقنية المعلومات	دور تقنية المعلومات للمؤسسة.
نموذج المصادر لتقنية المعلومات	نموذج المصادر الذي تتبناه المؤسسة لتقنية المعلومات كالاستعانة بمصادر خارجية.
طرق تنفيذ تقنية المعلومات	الأساليب التي تتبناها المؤسسة في تنفيذ تقنية المعلومات.
استراتيجية تبني التقنية	استراتيجية تبني التقنية في المؤسسة.
حجم المؤسسة	هل حجم المؤسسة هو مؤسسة كبيرة ام مؤسسة متوسطة.

مرفق رقم (٢)

(مجموع العمليات المصممة خصيصا للمصرف)

رمز العملية	اسم العملية	الغرض من العملية
EDM٠١	التأكيد على وضع إطار الحوكمة وصيانته	تقديم نهج متسق متكامل ومتوافق مع نهج إدارة المؤسسة. يتم اتخاذ القرارات المتعلقة بتقنية المعلومات بما يتماشى مع استراتيجيات وأهداف المؤسسة ويتم تحقيق القيمة المطلوبة. التأكد من أن العمليات المتعلقة بتقنية المعلومات يتم الإشراف عليها بشكل فعال وشفاف؛ تأكيد الامتثال للمتطلبات القانونية والتعاقدية والتنظيمية؛ واستيفاء متطلبات الحوكمة لأعضاء مجلس الإدارة.
EDM٠٣	التأكيد على تحسين المخاطر	التأكد من أن مخاطر المؤسسة ذات الصلة بـ التقنية المصاحبة لا تتجاوز قابلية المؤسسة وتحملها للمخاطر، وأن تأثير مخاطر التقنية المصاحبة على قيمة المؤسسة يتم تحديده وإدارته، وتقليل احتمالية فشل الامتثال.
APO٠٢	إدارة الإستراتيجية	دعم استراتيجية التحول الرقمي للمؤسسة وتقديم القيمة المرجوة من خلال خارطة طريق للتغييرات المتزايدة. استخدم نهج التقنية المصاحبة الشامل، مما يضمن أن كل مبادرة مرتبطة بوضوح بإستراتيجية شاملة. تمكين التغيير في جميع جوانب المنظمة المختلفة، من القنوات والعمليات إلى البيانات والثقافة والمهارات ونموذج التشغيل والحوافز.
APO٠٣	إدارة هيكلة المؤسسة	تمثيل اللبنات الأساسية المختلفة التي تشكل المؤسسة وعلاقاتها المتبادلة وكذلك المبادئ التي توجه تصميمها وتطورها بمرور الوقت، لتمكين التسليم القياسي والاستجابة والفعالة للأهداف التشغيلية والاستراتيجية.
APO٠٧	إدارة الموارد البشرية	تحسين قدرات الموارد البشرية لتحقيق أهداف المؤسسة.
APO٠٩	إدارة اتفاقيات الخدمة	التأكد من أن منتجات وخدمات ومستويات خدمة التقنية المصاحبة تلبي احتياجات المؤسسة الحالية والمستقبلية.
APO١٠	إدارة البائع	القيام بتحسين إمكانات التقنية المصاحبة المتاحة لدعم استراتيجية تقنية المعلومات وخريطة الطريق، وتقليل المخاطر المرتبطة بالموردين غير العاملين أو غير الممتثلين، وضمان الأسعار التنافسية.

APO١١	إدارة الجودة	ضمان التسليم المتسق للحلول والخدمات التقنية لتلبية متطلبات الجودة للمؤسسة وتلبية احتياجات أصحاب المصلحة.
APO١٢	إدارة المخاطر	دمج إدارة مخاطر المؤسسة ذات الصلة بـ T & I مع الإدارة الشاملة لمخاطر المؤسسة (ERM) وتحقيق التوازن بين تكاليف وفوائد إدارة مخاطر المؤسسة المتعلقة T & I.
APO١٣	إدارة الأمن	الحفاظ على تأثير ووقوع حوادث أمن المعلومات ضمن مستويات تقبل المخاطر في المؤسسة.
BAI٠١	إدارة البرامج	تحقيق قيمة الأعمال المطلوبة وتقليل مخاطر التأخير غير المتوقع والتكاليف وتآكل القيمة. للقيام بذلك، تحسين الاتصالات ومشاركة الأعمال والمستخدمين النهائيين، وضمان قيمة وجودة مخرجات البرنامج ومتابعة المشاريع داخل البرامج، وتعظيم مساهمة البرنامج في محفظة الاستثمار.
BAI٠٢	إدارة تعريف المتطلبات	القيام بإنشاء الحلول المثلى التي تلبي احتياجات المؤسسة مع تقليل المخاطر.
BAI٠٣	إدارة تحديد وبناء الحلول	ضمان تسليم سريع وقابل للتطوير للمنتجات والخدمات الرقمية. إنشاء حلول فعالة من حيث التكلفة وفي الوقت المناسب (التقنية وطريقة الأعمال وسير العمل) قادرة على دعم الأهداف الاستراتيجية والتشغيلية للمؤسسة.
BAI٠٤	إدارة التوافرية والقدرة	الحفاظ على توافر الخدمة والإدارة الفعالة للموارد وتحسين أداء النظام من خلال التنبؤ بمتطلبات الأداء والسعة المستقبلية.
BAI٠٦	إدارة تغييرات تقنية المعلومات	القيام بتمكين التسليم السريع والموثوق للتغيير في الأعمال. التخفيف من مخاطر التأثير السلبي على استقرار أو سلامة البيئة المتغيرة.
BAI٠٧	إدارة قبول تغيير تقنية المعلومات	تنفيذ الحلول بأمان وبما يتماشى مع التوقعات والنتائج المتفق عليها.
BAI٠٩	إدارة الأصول	حساب لجميع أصول التقنية المصاحبة وتحسين القيمة التي يوفرها استخدامها.
BAI١٠	إدارة التكوينات	توفير معلومات كافية حول أصول الخدمة لتمكين إدارة الخدمة بشكل فعال. تقييم تأثير التغييرات والتعامل مع حوادث الخدمة.
BAI١١	إدارة المشاريع	تحقيق نتائج المشروع المحددة وتقليل مخاطر التأخير غير المتوقع والتكاليف وتآكل القيمة من خلال تحسين الاتصالات ومشاركة الأعمال والمستخدمين النهائيين.

		ضمان قيمة وجودة مخرجات المشروع وتعظيم مساهمتها في البرامج المحددة والمحفظة الاستثمارية.
DSS٠١	إدارة العمليات	تقديم نتائج خدمات ومنتجات التقنية المصاحبة التشغيلية كما هو مخطط لها.
DSS٠٢	إدارة طلبات الخدمة والحوادث	تحقيق زيادة في الإنتاجية وتقليل الاضطرابات من خلال الحل السريع لاستفسارات المستخدم والحوادث. تقييم تأثير التغييرات والتعامل مع حوادث الخدمة. حل طلبات المستخدم واستعادة الخدمة استجابة للحوادث.
DSS٠٣	إدارة مشاكل الخدمة	زيادة التوافر وتحسين مستويات الخدمة وخفض التكاليف وتحسين راحة العملاء ورضاهم عن طريق تقليل عدد المشكلات التشغيلية وتحديد الأسباب الجذرية كجزء من حل المشكلة.
DSS٠٤	إدارة الاستمرارية	التكيف بسرعة ومواصلة الأعمال والحفاظ على توافر الموارد والمعلومات بمستوى مقبول للمؤسسة في حالة حدوث اضطراب كبير (على سبيل المثال، التهديدات والفرص والطلبات).
DSS٠٥	إدارة امن الخدمات	التقليل من تأثير الأعمال على نقاط الضعف والحوادث المتعلقة بأمن المعلومات التشغيلية.
DSS٠٦	إدارة ضوابط ممارسات الأعمال	الحفاظ على سلامة المعلومات وأمن أصول المعلومات التي يتم التعامل معها ضمن الأعمال في المؤسسة أو عملية الاستعانة بمصادر خارجية.
MEA٠٢	إدارة نظام الرقابة الداخلية	الحصول على الشفافية لأصحاب المصلحة الرئيسيين بشأن مدى كفاية نظام الضوابط الداخلية وبالتالي توفير الثقة في العمليات والثقة في تحقيق أهداف المؤسسة والفهم الكافي للمخاطر المتبقية.
MEA٠٣	إدارة الامتثال للمتطلبات الخارجية	التأكد من أن المؤسسة متوافقة مع جميع المتطلبات الخارجية المعمول بها.
MEA٠٤	إدارة الضمان	تمكين المؤسسة من تصميم وتطوير مبادرات ضمان تتسم بالكفاءة والفعالية، وتوفير التوجيه بشأن التخطيط وتحديد نطاق وتنفيذ ومتابعة مراجعات الضمان، باستخدام خارطة طريق تستند إلى مناهج ضمان مقبولة جيدًا.

مرفق رقم (٣)

منظومة السياسات (حد أدنى)

اسم السياسة	الغرض	النطاق
حوكمة تنظيم تقنية المعلومات والاتصالات	وضع القواعد والمعايير اللازمة لإدارة موارد تقنية المعلومات والاتصالات، بما في ذلك الشكل الإداري (مركزي او لا مركزي)، والهياكل التنظيمية بما في ذلك النشاطات والمهام والمسؤوليات لإدارة تلك الموارد، بما في ذلك الموارد المائية.	عمليات وخدمات ومشاريع تقنية المعلومات والاتصالات
أمن المعلومات وحمايتها	وضع القواعد والمعايير اللازمة لضمان متطلبات الحماية، السرية، والمصداقية، والتوافرية، والامتثال لإدارة موارد تقنية المعلومات والاتصالات بحسب المعايير الدولية المقبولة بهذا الشأن مثل (ISO-٢٧٠٠١/٢ IEC).	جميع المعلومات والتقنية المصاحبة لها
أمن بيانات بطاقات الدفع وحمايتها	اعتماد القواعد والمعايير اللازمة لضمان متطلبات الحماية، والسرية، والمصداقية، والتوافرية، والامتثال لإدارة أمن البيانات من قبل جميع الكيانات المشاركة في معالجة وإدارة بطاقات الدفع، بما في ذلك التجار، والمجهزين، والمؤسسات المالية، ومزودي خدمات الدفع الالكتروني، فضلاً عن جميع الكيانات الاخرى التي تقوم بتخزين، ومعالجة، او نقل بيانات حامل البطاقة و/ أو بيانات التصديق الحساسة بحسب المعايير الدولية المعتمدة بهذا الشأن واتخاذ جميع الاجراءات الفعلية للحصول على شهادة (PCI DSS) وفقاً لتلك المعايير.	بطاقات الدفع الالكتروني

خطط استمرارية العمل وخطط التعافي من الكوارث	وضع القواعد والمعايير اللازمة لبناء خطط التعافي من الكوارث وحماية الموظفين وخطط استمرارية الاعمال بما في ذلك اليات البناء والتشغيل والفحص والتدريب والتحديث على الخطط لضمان توافريه عمليات المؤسسة الحرجة.	عمليات المؤسسة الحرجة، وحماية البشر
أدارة مخاطر تقنية المعلومات والاتصالات	وضع القواعد والمعايير اللازمة لبناء مخاطر تقنية المعلومات والاتصالات بوصفها جزءاً من المخاطر الكلية للمؤسسة، بما في ذلك حوكمة تلك المخاطر والمسؤوليات والمهام المناطة بالأطراف المختلفة، وأليات تقييم وضبط ومراقبة المخاطر بهدف تعزيز العمليات اتخاذ القرار المبني على المخاطر وتحقيق اهداف المؤسسة.	جميع عمليات المؤسسة ومدخلاتها الخاصة بتقنية المعلومات والاتصالات.
امتثال تقنية المعلومات والاتصالات (IT Compliance)	وضع القواعد والمعايير اللازمة لضمان الامتثال لضوابط البنك المركزي والجهات الرقابية الأخرى، وللقوانين والانظمة السارية، ولسياسات المؤسسات.	جميع عمليات المؤسسة المعنية بموضوعات تقنية المعلومات والاتصالات
خصوصية البيانات (Data Privacy)	وضع القواعد والمعايير اللازمة لحماية البيانات الخاصة بالأشخاص الطبيعيين أو المعنويين من عمليات الافصاح والاستخدام غير المصرح به.	البيانات الخاصة كافة
الاستعانة بخبرات خارجية (Outsourcing)	اعتماد سياسة عامة للاستعانة بالموارد بشكل عام وبموارد تقنية المعلومات والاتصالات بشكل خاص؛ تلك الموارد سواء مملوكة للمؤسسة (In-sourcing) أو مملوكة للغير (Outsourcing) تراعي الضوابط والانظمة والقوانين وتحاكي افضل الممارسات الدولية المقبولة بهذا الشأن ؛ وتأخذ بالحسبان مكان العملية الانتاجية (On-site Near-site Off-shore Off site) وتأخذ بالحسبان وتراعي متطلبات مراقبة مستويات الخدمة	عمليات المؤسسة كافة

	(Service Levels) وتفعيل حق التدقيق (Audit Right) من قبل اطراف ثالثة محايدة موثوقة فضلا عن متطلبات الكفاءة والفعالية في استغلال الموارد.	
أدارة محفظة المشروع (Project Portfolio Management)	وضع القواعد والمعايير اللازمة لإدارة المشاريع بما في ذلك مراحل المشروع والحوكمة اللازمة لتحقيق المتطلبات المتعلقة بالجودة(Quality Requirements) وتلك المتعلقة بالحماية والسرية (Confidentiality Requirements)وتلك المتعلقة بالامتثال تحقيقاً لأهداف المؤسسة وعملياتها.	جميع مشاريع المؤسسة المتعلقة بتقنية المعلومات والاتصالات
إدارة الموجودات (Asset Management)	وضع القواعد والمعايير اللازمة لتصنيف درجة مخاطر البيانات والانظمة المختلفة وتحديد مالكيها وضوابط حمايتها خلال مراحل دورة حياتها المختلفة.	البيانات والاجهزة والبرامج والادوات المصاحبة لها.
الاستخدام المقبول لموارد تقنية المعلومات والاتصالات	وضع القواعد والمعايير اللازمة لتحديد السلوك المقبول وغير المقبول لموارد تقنية المعلومات والاتصالات	الاجهزة والبرامجيات والتطبيقات والشبكات بما في ذلك الانترنت والبريد الالكتروني
إدارة التغيير (Change Management)	وضع القواعد والمعايير اللازمة لضمان مصداقية التغيير من حيث توثيق الموافقات اللازمة من مالكي الاصول الخاضعة للتغيير.	جميع عمليات تقنية المعلومات والاتصالات
اجهزة الحواسيب الرئيسية Servers	وضع قواعد ومعايير لتقليل عمليات النفاذ والاستخدام الغير مشروع للأجهزة بما في ذلك ضوابط نفاذ موظفي دائرة تقنية المعلومات والاتصالات وذوي الامتيازات العليا لبيئات التشغيل فضلا عن معايير إدارة عمليات التشغيل اليومي للأجهزة والبرامجيات المختلفة بما في ذلك ضوابط الحماية وأليات المراقبة والصيانة الدورية لتلك الاجهزة.	جميع الحواسيب الرئيسية المملوكة او المدارة من قبل المؤسسة لكل بيئات التطوير والفحص والتشغيل بما في ذلك نظم التشغيل والادوات الاخرى المصاحبة لها.

اجهزة الكمبيوتر الطرفية	وضع قواعد ومعايير سلوكية وتقنية لضمان حماية البيانات الحساسة المخزنة على الأجهزة.	كل الاجهزة الطرفية المرتبطة بالشبكات أو القائمة بحد ذاتها
الأجهزة المحمولة	وضع قواعد ومعايير سلوكية وتقنية لضمان حماية البيانات الحساسة المخزنة على الأجهزة.	كل الاجهزة المحمولة مثل (Smart Laptop, PDA Phone, USB, Memory Cards .....Etc.)
إدارة صلاحيات وامتيازات النفاذ (User Access Management)	وضع قواعد ومعايير لضمان منح صلاحيات وامتيازات النفاذ للبيانات والبرامج والاجهزة لمستخدميها بحسب الحاجة للعمل وبالحد الأدنى بما يكفل السرية والمصداقية والتوافرية لموارد تقنية المعلومات والاتصالات.	كل البرامج والاجهزة وقواعد البيانات وما هو في حكمها
تطوير / اقتناء الانظمة والبرامجيات (System Development Life Cycle)	وضع القواعد والمعايير اللازمة لتنفيذ مراحل تطوير / اقتناء الانظمة والبرامجيات المختلفة لضمان تلبيتها لمتطلبات العمل من خلال منهجيات التطوير المختلفة المتناسبة مع متطلبات العمل وأهدافه.	كل الاتفاقيات والتعاقدات والالتزامات مع الاطراف الخارجية والاطراف من داخل المؤسسة.
إدارة مستوى الخدمة (Service Level Management)	وضع قواعد ومعايير لتحديد مستوى الخدمة المقدمة وقبولها وتوثيقها وقياسها ومراقبتها وتحسينها سواء من أطراف داخلية أم أطراف خارجية لضمان الاستغلال الامثل للموارد ودعم عمليات المؤسسة المختلفة.	كل الاتفاقيات والتعاقدات والالتزامات مع الاطراف الخارجية والاطراف من داخل المؤسسة.
النسخ الاحتياطي والاسترجاع (Back-up and Restore)	وضع قواعد ومعايير لأليات النسخ الاحتياطي والاسترجاع لضمان توافريه البيانات ومصداقيتها وسريتها.	البيانات في بيئات التشغيل وحيثما يلزم
الاحتفاظ بالبيانات (Data Retention)	وضع قواعد ومعايير الخاصة بحجم البيانات الواجب توافرها سواء بشكل ورقي أو تلك المتواجدة على اجهزة الحواسيب والتطبيقات المختلفة والمدة الزمنية الواجب	كل الاجهزة والبرمجيات ووسائل وادوات الاحتفاظ بالبيانات.

	الاحتفاظ بها والمفاضلة بين حجم البيانات المتوافرة وسرعة الاداء في الوصول الى البيانات	
شراء الانظمة والتجهيزات (Purchasing Systems)	وضع قواعد ومعايير للمفاضلة بين المزودين الخارجيين	كل التجهيزات التقنية والبرامج المتعلقة بها.
النفاذ عن بعد (Remote Access)	وضع قواعد ومعايير للربط الشبكي عن بعد بشبكات الحواسيب الخاصة بالمؤسسة لتقليل مخاطر الاطلاع والاستخدام لبيانات ومصادر المؤسسة الحساسة ولأنظمة الضبط والرقابة الداخلية المعنية بحماية موجودات المؤسسة وللحماية من مخاطر السمعة.	الاطراف والشركاء الداخليين والخارجيين مثل مزودي الخدمات ولجميع بيئات التطوير والفحص والتشغيل للأجهزة والشبكات ومنها على سبيل المثال لا الحصر شبكات الانترنت والشبكات المشفرة وخطوط الاتصال المختلفة مثل (Frame Relay, ISDB, VPN, DSL, MPLS)
الشبكات (Networks)	وضع قواعد ومعايير لضمان تحقيق متطلبات الكفاءة والفعالية في استغلال عناصر الشبكات والاتصالات من جهة وتحقيق متطلبات الامن والحماية من جهة اخرى دعما لتحقيق اهداف المؤسسة.	كل عناصر الشبكات بجميع البيئات
الشبكات اللاسلكية (Wireless Networks)	وضع قواعد ومعايير بغرض حماية البيانات الحساسة المتناقلة عبر الشبكات اللاسلكية من الاعتراض والاستخدام الغير مشروع.	كل الشبكات اللاسلكية الفعلية منها والافتراضية

الجدران النارية (Firewalls)	وضع الحد الادنى من القواعد والمعايير المنظمة لألية عمل اجهزة الجدران النارية (firewalls) وألية حمايتها لتفعيلها بالشكل المطلوب والكفيل بحماية وضمان سرية ومصداقية بيانات وعمليات المؤسسة وتوافريها.	كل اجهزة ال (firewalls) العاملة بالبيئات كافة مثل (DNS, Proxy, External DNS, VPN, Routers, Switches servers .... etc.)
فحص الاختراق وتحليل الثغرات (penetrating testing and vulnerability assessment)	وضع قواعد ومعايير لفحص الاجهزة وعناصر الشبكات لضمان عدم وجود ثغرات أمنية تُمكن من اختراق البيانات والانظمة والعمليات الحساسة للمؤسسة.	كل موجودات المؤسسة التقنية من اجهزة حواسيب رئيسية وحماية عناصر الشبكات والبرمجيات.
مقسم الهاتف الخاص (Private Branch Exchange)	وضع الحد الادنى من قواعد ومعايير الحماية لأنظمة المقسم لضمان الحماية والسرية لبيانات وعمليات المؤسسة من الاستخدام غير المشروع.	كل اجهزة القسم المملوكة وغير المملوكة للمؤسسة

مصرف اربيل للاستثمار والتمويل
شركة مساهمة خاصة
الادارة العامة

مرفق رقم (٤)

المعلومات والتقارير (حد أدنى)

أسم التقرير	محتوياته
مصفوفة الصلاحيات والامتيازات (Authority Matrix)	مصفوفة تحدد الصلاحيات والامتيازات الممنوحة على جميع البرامج وقواعد البيانات وعناصر الشبكات؛ مثل التفاصيل اسم المستخدم ووظيفته وصلاحيته أو امتيازاته.
تحليل عوامل مخاطر تقنية المعلومات والاتصالات (IT Risk factors Analysis)	١-التهديدات الداخلية. ٢- التهديدات الخارجية. ٣- مواطن الضعف في إدارة موارد تقنية المعلومات والاتصالات. ٤- مواطن الضعف في قدرة تقنية المعلومات والاتصالات على تمكين عمليات المؤسسة. ٥- مواطن الضعف في إدارة مخاطر تقنية المعلومات والاتصالات.
تحليل سيناريو مخاطر تقنية المعلومات والاتصالات (IT Risk Scenario Analysis)	١- مصدر التهديد إما داخلي او خارجي. ٢- نوع التهديد (Threat Type) مثل الاخطاء، أو اختراق فيروس، أو احداث خارجية. ٣- الحادث (Event): مثل الافصاح عن معلومات سرية، أو تعطل أو تعديل غير مشروع، أو سرقة وتدمير أو تصميم غير فعال للقوانين والانظمة أو الاستخدام غير المقبول. ٤- الأصول المتأثرة (Asset or Recourse Affected): مثل بشر أو هياكل تنظيمية لعمليات البنية التحتية لتقنية المعلومات، أو معلومات برامج. ٥- الوقت: وقت الحدوث، مدة الحادث، عمر الحادث قبل اكتشافه.

سجل مخاطر تقنية المعلومات والاتصالات (IT Risk Register)	١- مقدمة: مالك الاصل، فريق التقييم، تاريخ التقييم اللاحق، مُلخص تقييم المخاطر، وخيار ادارة المخاطر. ٢- سيناريو تحليل مخاطر تقنية المعلومات والاتصالات في اعلاه. ٣- تقييم مخاطر تقنية المعلومات والاتصالات من حيث احتساب محوري المخاطر المتمثلة باحتمالية الحادث (Potentiality)، وحجم الأثر (Impact or Severity)، وبفصل استخدام مقياس معياري زوجي لمحاور التقييم، وإظهار حجم الأثر استناداً الى اهداف وعمليات المؤسسة المتضمنة تقنية المعلومات والاتصالات باستخدام محاور التقييم لأحد النماذج العالية الاتية على سبيل المثال: أ- COBIT Information Criteria ب- COBIT for Risk ت- Balanced Scorecard (BSC) ج- Extended BSC د- Westerman ه- COSO ERM و- FAIR (Factor Analysis of Information Risk) ٤- قابلية تحمل المخاطر (Risk Appetite). ٥- خيار إدارة المخاطر (مقبول (في حالة كانت كمية المخاطر المحسوبة اقل من قابلية تحمل المخاطر)، تخفيف تجنب تحويل). ٦- بنود خطة إدارة المخاطر ومتابعتها (نُفذت، أو قيد التنفيذ بحسب الخطة). ٧- معايير اداء رئيسية لمراقبة مستوى المخاطر (Key Risk Indicators) للتأكد من عدم تجاوز قابلية تحمل المخاطر ودرجة تحمل المخاطر (نسبة الانحراف الموجب للقابلية تحمل المخاطر).

RACI Chart	قوائم تتضمن تحييد الجهة أو الجهات أو الشخص أو الاطراف المسؤولة بشكل اولي (Responsible) وتلك مسؤولة بشكل نهائي (Accountable) ، وتلك المستشارة (Consulted) وتلك التي يتم اطلاعها (Informed) لكل عمليات ادارة موارد تقنية المعلومات والاتصالات ؛ وإدارة مخاطر وأمن المعلومات والرقابة المستقلة .
ملف المخاطر (IT Risk profile)	١- سجل المخاطر. ٢- تحليل عوامل المخاطر. ٣- الخسائر المتحققة وغير المحققة (Losses and Near – Misses). ٤- تدقيق جهات مستقلة.
تقارير المخاطر (IT Risk Report)	يوضح كمية مخاطر تقنية المعلومات والاتصالات الحالية المتضمنة في عمليات المؤسسة؛ والاجراءات المتخذة أو التي سيتم اتخاذها لإدارة تلك المخاطر؛ ويتم تصميم شكل وطريقة عرض هذه التقارير بحيث تخدم متخذ القرار مالك العملية / العمليات التي تقع ضمن مسؤوليته حسب طلبه.
خريطة المخاطر (IT Risk Map or Heat map)	رسم بياني يوضح محوري المخاطر (الاحتمالية والاثر) ومناطق المخاطر المقبولة وغير المقبولة بحسب قابلية تحمل المخاطر بموجب ألوان تساعد على توضيح ذلك، وتؤشر عليه مخاطر تقنية المعلومات والاتصالات المحسوبة والموجودة في عمليات ذلك.
Risk Universe Appetite and Tolerance	تقرير يوضح جميع المخاطر المتضمنة في العملية بما فيها مخاطر تقنية المعلومات والاتصالات، يوضح كمية المخاطر المخطط قبولها (Risk Appetite)ونسبة الانحراف الموجب على قابلية تحمل المخاطر (Risk Tolerance).
مؤشرات قياس المخاطر الرئيسة (Key Risk Indicator)	عبارة عن معايير قياس يتم تحديدها ومقارنتها ب (Benchmark)لمراقبة المخاطر الحالية للتأكد من عدم تجاوزها للقابلية على تحمل المخاطر، ويتم تحديدها لتكون مؤشرات قياس استناداً الى المعايير الآتية: أ- الأثر: حصة وحجم المؤثر في قياس اثر المخاطر. ب- القابلية للقياس. ج- الاعتمادية. د- الحساسية

Risk Taxonomy	توضيح معاني المصطلحات المستخدمة في تعريف وقياس وإدارة ومراقبة المخاطر، فضلاً عن معايير قياس المخاطر والتعبير عنها، بحيث يتم استخدام تلك المصطلحات بالمعنى والمفهوم ذاتيهما لدى جميع الشركاء، وبما يتفق وضوابطنا بهذا الشأن.
Risk and Control Activity Matrix (RCAM)	مصفوفة تبين كمية المخاطر المحسوبة والاجراءات والضوابط المقابلة المتخذة لإدارة تلك المخاطر ومدى كفايتها، والسيطرة عليها.
موازنة أمن المعلومات وحمايتها	يتم تحديد المصاريف المخطط لإنفاقها على امن المعلومات للعام القادم ضمن الموازنة العامة للمؤسسة وبما يتوافق والمشاريع المُخطط لتنفيذها، متضمنة تحليل الانحراف القائم لمصاريف العام الحالي مقارنة مع الموازنة المحددة للعام نفسه.
MIS report	مصفوفة تبين جميع انواع التقارير المنتجة بحيث تظهر اسم مالك التقرير، ووظيفته، ودورية انتاجه، والإجراء المتخذ تجاهه.
استراتيجية أو منهجية تدقيق تقنية المعلومات والاتصالات (Audit strategy)	يتم تحديد اهداف تقنية المعلومات والاتصالات ونطاق التدقيق وبرامج التدقيق المستخدمة في عمليات المراجعة.
ميثاق تدقيق تقنية المعلومات والاتصالات (IT Audit Charter) (Engagement Letter)	ميثاق مستقل أو ضمن الميثاق العام للتدقيق الداخلي يتم فيه تحديد صلاحيات عمل تدقيق تقنية المعلومات والاتصالات، ومسؤولياته، وطبيعته، ونطاقه، وبما يتفق وضوابطنا بهذا الشأن ويتم تضمين ال (Engagement Letter) الموقعة مع المدقق الخارجي بذلك ايضاً.
خطة تدقيق تقنية المعلومات والاتصالات (IT Audit Plan)	يتم رسم خطة مستقبلية للتدقيق تكون مرتكزة ومبنية على المخاطر.
مصفوفة المؤهلات (HR Competencies)	تتضمن الشهادات الاكاديمية والمهنية والفنية ومجموع الخبرات والمهارات اللازم امتلاكها لكوادر إدارة تقنية المعلومات والاتصالات، والتشغيل، وتدقيق تقنية المعلومات والاتصالات، وأمن المعلومات وحمايتها.
سجل تدقيق تقنية المعلومات والاتصالات (Assurance Finding Register)	يحتوي جميع نقط وملحوظات التدقيق والاجراءات والمتابعات المتخذه حيالها.

ملف تدقيق تقنية المعلومات والاتصالات (Assurance Report Repository)	يحتوي كل تقارير تدقيق تقنية المعلومات والاتصالات.
أفضل المعايير الدولية لإدارة موارد ومشاريع تقنية المعلومات والاتصالات وإدارة مخاطر تقنية المعلومات والاتصالات وأمن وحماية والتدقيق على تقنية المعلومات والاتصالات	يتم انشاء مكتبة بالمراجع المطلوبة بحسب أفضل الممارسات الدولية وتوفير استخدامها لكادر المؤسسة بحسب طبيعة العمل، فضلاً عن منظومة القوانين والانظمة والضوابط المراعاة.