مصرف ليبيا المركزي

ص.ب 1103 العنوان البرقي : مصرفليبيا - طرابلس - ليبيا

الإشاري: ا.ر.م.ن 804

المنشور أ ر م ن رقم (21/ 2023)
التاريخ: 22 ذو الحجة 1444
الموافق: 10 يوليو 2023

السادة / رؤساء مجالس الإدارة و المُدراء العامون للمصارف
السادة / رؤساء مجالس الإدارة و المُدراء العامون للمصارف المُتَخَصِّصة
السادة / مُدرآء شركات مُزَوِّدي خدمة الدفع الإلكتُروني

الموضوع: دليل حوكمة تكنولوجيا المعلومات

****

تأسيساً على أحكام القانون رقم (1) لعام 2005 بشأن المصارف وتعديله، وإعمالاً بالدور الإشرافي والرقابي لمصرف ليبيا المركزي، وتْعّزيزاً لمبدأ الإدارة المؤسسية الفعّالة لتكنولوجيا المعلومات.

وبالإشارة إلى المنشور أ. ر. م. ن . (2010/13) الصادر في 27 سبتمبر 2010، بِشأن تعميم قرار مجلس إدارة مصرف ليبيا المركزي رقم (20) لسنة 2010 بإعتِماد دليل الحوكمة للقِطاع المصرفي الليبي.

عليهِ، نرفق لَكُم دليل حوكمة تكنولوجيا المعلومات، الّذي يُمَثِّل إطار عام لحوكمة وإدارة المعلومات والتكنولوجيا المُصاحِبة لها، والمبادئ التوجيهية لإدارة مخاطر تكنولوجيا المعلومات، وأمن البيانات، والأمن السيبراني لدى المصارف والمؤسسات المالية الخاضعة لرقابة مصرف ليبيا المركزي، وذلك للعمل به ووضعه موضع التنفيذ وفق الإستراتيجية التالي: تُعتبر الستة أشهُر من النصف الثاني لهذا العام 2023 مرحلة أوّليّة يتم فيها رفع مُستوى الوعي بما ورد من تعليمات بالخُصوص، وكذلك تهيئة وتأهيل البُنى التحتية لتكنولوجيا المعلومات. ثُم تكون الستة الأشهُر الأولى من النصف الأول من عام 2024 مرحلة البدء في تقييم وتنفيذ التعليمات المُتعلقة بِحوكمة تقنية المعلومات. ولتكون الستة أشهُر من النصف الثاني لعام 2024 مرحلة الشُروع في تقييم وتنفيذ ماورد من تعليمات تتعلّق بحوكمة الأمن السيبراني ومافي حُكمِهِ، وستقوم إدارة الرقابة على المصارف والنقد بِمُتابعة الموضوع من خلال المهام التفتيشية للتأكُّد من مدى إمتثال مؤسَّساتِكُم لما وَرَدَ فيهِ.

والسلام عليكم ،،،

ناجي محمد عيسى
مدير إدارة الرقابة على المصارف والنقد

صورة لكل من:
السيد / المحافظ
السيد / نائب مدير إدارة الرقابة على المصارف والنقد لشؤون الرقابة المكتبية ومراقبة الامتثال
السيد / نائب مدير إدارة الرقابة على المصارف والنقد لشؤون التفتيش
السيد / نائب مدير إدارة الرقابة على المصارف والنقد لشؤون الصيرفة الإسلامية
السادة/ الرقابة المصرفية بنغازي
السادة / رؤساء وحدات الإمتثال بالمصارف (للمتابعة)

مصرف ليبيا المركزي
CENTRAL BANK OF LIBYA

إدارة الرقابة على المصارف والنقد
Banking Supervision Department

دليل حوكمة تكنولوجيا المعلومات

IT Governance Guideline

قائمة المحتويات

قائمة المصطلحات

حوكمة تكنولوجيا المعلومات	توزيع الأدوار والمسؤوليات بين الأطراف والجهات المُختلفة وأصحاب المصلحة (مثل المجلس والادارة التنفيذية) باتباع النهج الأمثل الذي يكفل الموازنة بين المخاطر والعوائد المُتوقعة، من خلال إعتماد القواعد والأُسس والآليات اللازمة لصنع القرار وتحديد التوجهات الإستراتيجية والأهداف في المؤسسة وآليات مُراقبة وفحص إمتثال مدى تحققها بما يكفل ديمومة وتطور المؤسسة.
COBIT	إطار عمل حوكمة تكنولوجيا المعلومات تم إنشاءه من قبل جمعية المدققين التقنيين الأمريكية.
ISACA	جمعية المُدققين التقنيين الأمريكية.
عمليات حوكمة تكنولوجيا المعلومات	مجموعة المُمارسات والنشاطات المُنبثقة عن سياسات المؤسسة واللازِمة لتحقيق أهداف المعلومات والتكنولوجيا المصاحبة لها.
المؤسسة المالية	أي من المصارف وشركات مُزودي خدمات الدفع الإلكتُروني وشركات الصِرافة والشركات المُساهِمة العامة والخاصة المُرَخَّص لَها بِمُزاولة خدمات الدفع أو إدارة وتشغيل أنظمة الدفع الإلكتُروني.
المجلس	مجلس إدارة المؤسسة وما في حُكْمِهِ.
الإدارة التنفيذية	تشمُل المُدير العام ومُدير العمليات ومُعاون المُدير المُفوض ومُدير إدارة المخاطر ومُدير الإمتثال بالإضافة ألي موظف في المؤسسة له سُلطة تنفيذية، ويرتبط وظيفياً مُباشرةً بالمدير العام.
بيئة تكنولوجيا المعلومات	مجموعة من التجهيزات الحاسوبية الخاصة بالشبكات الداخلية والشبكات الخارجية والخوادم الرئيسية والبرمجيات العاملة عليها، وجميع الأجهزة المُساندة لها في الموقع الرئيسي والبديل.
المعلومات Information	أية بيانات شفوية أو مكتوبة أو سجلات أو إحصائيات أووثائق مكتوبة أو مصورة أو مسجلة أو مخزنة إلكتُرونياً، أو أية طريقة أخرى تُعد ذات قيمة للمؤسسة.
البيانات Data	الحقائق الخام التي يُمكن توضيحُها بالحُروف والأ{قام ومن المُمكن أن تُمثل الأشخاص أو الأشياء أو الأحداث.
أصول المعلومات Information Assets	أيّة معلومات أو ملفات إلكتُرونية أو غير إلكتُرونية أو أجهزة أو وبائط تخزين أو برامج أو أيٍّ من مُكونات لبيئة تكنولوجيا المعلومات والإتصالات المُتعلقة بأعمال المؤسسة.
الهُجوم السيبراني Cyber Attack	أيّة مُحاولة تدمير أو كشف أو تغيير أو تعطيل أو سرقة أو مُحاولة إستغلال نُقط ضعف أو نفاذ غير مشروع لأصول معلومات المؤسسة ضمن الفضاء السيبراني.
الأمن السيبراني Cyber Security	الحفاظ على سرية وتكامُلية وتوافرية المعلومات وأصول المعلومات التابعة للمؤسسة ضمن الفضاء السيبراني من أيّ تهديد سيبراني، عن طريق مجموعة من الوسائل والسياسات والضوابط و أفضل المُمارسات بهذا الشأن.
التهديد السيبراني Cyber Threat	ظرف أو حدث يحتمل أن يستغل (عن قصد أو غير قصد) واحدة أو أكثر من نقط الضعف الموجودة في بيئة تكنولوجيا المعلومات والإتصالات بالمؤسسة، مِمّا يؤثر في أمنها السيبراني.
الحدث السيبراني Cyber Event	أيّة واقعة تدل على وجود تهديد سيبراني على بيئة تكنولوجيا المعلومات والإتصالات للمؤسسة.
المخاطر السيبرانية Cyber Risks	مقدار ترجيح ناتج عن إحتمال وقوع حدث سيبراني في نطاق أصول المعلومات للمؤسسة، و أثر ذلك الحدث في المؤسسة.

الحوكمة السيبرانية Cyber Governance	ترتيبات المؤسسة لوضع وتنفيذ ومُراجعة نهجِها لإدارة المخاطر السيبرانية.
إدارة المخاطر السيبرانية Cyber Security Management	عمليات تحديد وقياس وضبط ومُراقبة المخاطر السيبرانية.
حوكمة البيانات Data Governance	عملية إدارة توافُرية البيانات المستخدمة في المؤسسة، وأمنها، وسهولة إستخدامها، وسلامتها.
الشفرات الضارة أو الخبيثة Malicious Codes	برمجيات أو ملفات ضارة تتضمن وظائف لها قُدرات تؤثر بشكل سلبي، سواء بشكل مباشر أو غير مباشر في بيئة تكنولوجيا المعلومات والإتصالات.
الحماية Protection	توظيف الإجراءات والضوابط والتدابير المُلائمة لتقديم خدمات وأعمال المؤسسة بصورة موثوقة.
الكشف Detection	توظيف الضوابط والإجراءات المُناسبة من أجل العلم بوقوع الحدث السيبراني فوراً.
الإستجابة Response	توظيف الضوابط والإجراءات المُناسبة لإحتواء الحدث السيبراني عند كشفه.
الإستعادة Restore	عملية إسترجاع المعلومات المُخزنة على وسائط النسخ الإحتياطية، عند تلف أو فُقدان المعلومات الأصلية، أو الحاجة إليها بعد مثدّة من الزمن لإعادة سير عمل المؤسسة.
التعافي Recovery	مجموعة من الإجراءات التي يتم إتخاذُها و إتباعُها لإعادة الأعمال في المؤسسة إلى وضعها الطبيعي، وإعادة تشغيل موارد التكنولوجيا المُتعددة في تشغيل عمليات المؤسسة إلى ما كانت عليه قبل وقوع الحدث.
نقط الضعف Vulnerabilities	خلل أو نقص في ضوابط الحماية المُستخدمة في أي من مكونات بيئة تكنولوجيا المعلومات والإتصالات المتعلقة بأعمال المؤسسة الممكن إستغلالها في عمليات الإختراق والهُجوم السيبراني.
ضوابط الوصول / النفاذ Access Control	القواعد والآليات المُستخدمة للسماح بإستخدام أصول المعلومات، ونفاذ الأشخاص المخولين فقط إليها، وبما يتوافق وطبيعة مسءولياتِهم في المؤسسة.
الإمتيازات والصلاحيات Privileges	مُستوى الصلاحيات التي يتم منحها للمُستخدمين للوصول للنفاذ وإستخدام أي من مُكونات بيئة تكنولوجيا المعلومات بالمؤسسة.
إدارة التغيير Change Management	إدارة وضبط وتوثيق أي تغيير يتم إجراؤه على أي من مثكونات بيئة تكنولوجيا المعلومات في المؤسسة، أو أي تغيير في الإجراءات المعمول بها في المؤسسة من قبل الأطراف المُخَوَّلة بالموافقة.
تصنيف المعلومات Information Classification	تحديد مُستوى الحسّاسية المُناسب للمعلومات التي يتم إنشاؤها أو تغييرها أو نقلها أو تعديلها أو حفظها على أيّة وسائل كانت وبأيّة تقنيات مُمكنة، إستناداً إلى المخاطر المُترتبة على الاطلاع والاستخدام غير المشروع لتلك المعلومات.
السرية Confidentiality	حماية المعلومات من عمليات الاطلاع والنشر والإفصاح والاستخدام غير المشروع.
التوافرية Availability	إمكانية استخدام والوصول إلى المعلومات والانظمة في المؤسسة، وإسترجاعها عند الطلب.
التكامُلية Integrity	دقة وإكتمال وسلامة المعلومات أو نُظُم المعلومات، أو أيّ جُزء منها والتحقق من أنَّهُ لم تطرأ عليها أيّة زيادة أو نُقصان أو تغيير غير مشروع.
المُلاءمة Appropriate	توافر الحد الأدنى من المُتطلبات لأعضاء مجلس إدارة المصرف/الشركة، وهيأة الرقابة الشرعية في المصرف الإسلامي، وأعضاء الإدارة التنفيذية.

المبادئ التوجيهية Guidelines	عِبارة عن قائمة بأفضل المُمارسات في القطاع المصرفي، التي من المُتَوَقع أن تعتمدها المؤسسة.
زمن التعافي المُستهدف Recovery Time Objective	أقصى وقت مسموح به لإعادة تشغيل الخدمة أو العملية بعد حُدوث الإنقطاع في الخدمة.
نقطة الإسترجاع المُستهدفة Recovery Point Objective	هو العمر الأقصى المسموح للبيانات التي قد تفقد عند إستعادة الخدمة، بعد حُدوث إنقطاع.
العمليات الحرجة Critical Operation	العمليات التي لا يُمكن تحمُّل توقفها لمدد زمنية طويلة بحسب دراسات تحليل الأثر على الأعمال في المؤسسة، وتلك العمليات ذات المخاطر والأهمية النسبية للمؤسسة.
التشفير Encryption	عملية تحويل المعلومات إلى شكل غير مقروء أو مفهوم.
الطرف الثالث Third Party	الجهة التي تعهد إليها المؤسسة تولّي الأعمال الفنية والتقنية بشكل كُلّي أو جُزّئي، لمساعدتها على القيام بالأعمال المُرخّصة بها، بما لا يتعارض مع أحكام التشريعات النافذة.
أصحاب المصالح Stakeholders	أي ذي مصلحة في المؤسسة، مثل المُساهمين أو الموظفين، أو الدائنين أو الزبائن أو المزودين الخارجيين، أو الجِهات الرقابية المعنية.
الاسناد الخارجي Outsourcing	الاستعانة بطرف ثالث أو توظيف موارده، لتسيير أعمال المؤسسة أو جُزء من أعمالها التي تقع ضمن مسؤولياتها.
الأمن المادي Physical Security	المعايير وإجراءات الحماية التي تر اقب أو تحدد الدخول إلى أي من مر افق المؤسسة، أو مواردها، أو معلومات المؤسسة المُخَزَّنة على وسائط: فيزيائية لمنع الوصول إلى الموارد المعلوماتية والأنظمة، مثل المباني وخز ائن الملفات، والأجهزة المكتبية والمحمولة والخوادم والمُعِدّات.
سجلات التدقيق Audit Trail	ملفات بيانات تقدم أدلة مستندية على تسلسل العمليات الوظائفية والإدارية التي تحدث على الأنظمة.
تقييم المخاطر Risks' Assessment	قياس وتحديدإحتمالية حُدوث المخاطروشدتها، وتوقع مقدارتأثيرها على المؤسسة.
أختبارات الاختراق Penetration Testing	أختباريحاول فيه المختصون البحث عن الثغرات الأمنية والتحايل على الخصائص الأمنية لأنظمة المعلومات والضو ابط الأمنية واستغلالها لمحاولة اختراق تلك الانظمة من خارج أوداخل المؤسسة، لمعرفة مدى فعالية الضو ابط الأمنية المُستخدمة من قبل المؤسسة لحمياة أنظمتها.
DAS	Direct Attached Storage وهي وسيلة التخزين الرقمي المُتصلة مباشرة بالكمبيوتر، مثل محركات الأقراص الصلبة، والاقراص الثابتة، ومُحركات الأقراص الضوئية.
NAS	Network Attached Storage وهو وحدة التخزين الشبكي، لتخزين بيانات الكمبيوتر على الشبكة لتوفير الوصول إليها لأكبر عدد ممكن من أجهزة المستخدين الأخرى، أو الزبائن المتصلة بالشبكة نفسها.
SAN	Storage Area Network وهو نظام تخزين مُخَصّص عالي الأداء، يقوم بنقل بيانات مُستوى الكتلة بين الخوادم وأجهزة التخزين، عادةً ما يتم إستخدام SAN في مر اكز البيانات أو المؤسسات أو بيئات الحوسبة الإفتراضية.

أولاً: المُقدمة:

في الآوِنة الأخيرة، كان قطاع تكنولوجيا المعلومات عُنّصُراً أساسياً في أعمال المؤسسات سواءً الشركات أو المصارف، حيثُ أصبح قطاع تكنولوجيا المعلومات يؤدي دوراً محورياً، وتدل الأبحاث أن له دور بارز في إتاحة المزيد من فُرص زيادة دخل المؤسسة وسُهولة الحُصول على المعلومات ودعم خدمات البُنية التحتية، وكذلك سُهولة إجراء العمليات التجارية أو الخدمية، فضلاً عن السرعة في إجرائها وتحسين جودة المُنتجات والخدمات وزيادة الناتج الإجمالي. ومِمّا لا شك فيهِ أن المؤسسات بجميع أنواعها تواجه العديد من التَغَيُّرات والتحديات التي فرضتها تكنولوجيا المعلومات، ودعت كل هذه التحديات والتغيرات الى ظُهور مفهوم جديد يتعلق بِأستخدام تكنولوجيا المعلومات في المؤسسات وهو مفهوم حوكمة تكنولوجيا المعلومات، ولعل إستخدام المؤسسة لمفهوم حوكمة تكنولوجيا المعلومات بشكل جيد من شأنه أن يُحقق لها أهدافها والموائمة بين فوائد تكنولوجيا المعلومات ومخاطرها.

مع التطور الحاصل في تكنولوجيا المعلومات وإعتماد الأعمال ومن ضمنها القطاعات المالية على التكنولوجيا الناشئة، وما أحدثه توافر تكنولوجيا المعلومات و تطوره، ظهرت الحاجة إلى رفع مُستوى الأدآء بِأستخدام تكنولوجيا المعلومات والتكنولوجيا المُصاحبة على مُستوى المؤسسسات العاملة في مُختلف المجالات وذلك بأتباع أفضل السبل العلمية والمعايير الدولية والأطر العالمية في إدارة تكنولوجيا المعلومات، ومن هذا المُنطلق تطورت تكنولوجيا المعلومات والاتصالات وأدت إلى تغييرات سريعة في الطريقة التي تتم بها الأعمال والعمليات في القطاعات المصرفية، ولم تَعُد تكنولوجيا المعلومات والاتصالات وظيفة دعم داخل المؤسسات المالية فحسب، بل أصبحت عامل تمكين أساسي لإستراتيجيات الأعمال، بما في ذلك الوصول إلى إحتياجات الزبائن وتلبيتها، من خلال توفير وإدامة الخدمات التقنية وفقاً لأنسب المعايير الدولية، وأفضل الممارسات للحفاظ على جودة المعلومات، وكذلك من خلال مواكبة التطورات التقنية وتنمية قدرات ومهارات الموارد البشرية، بشكل يؤدي إلى تحقيق أهداف القطاع المصرفي الليبي الواردة في قانون المصارف النافذ.

وكذلك فقد تطورت الأنظمة المصرفية، والشبكات التي تدعم العمليات التجارية للمؤسسات من حيث النطاق والتعقيد على مرّ السنين، ويمكن للمؤسسات المالية التي تقدم مجموعة مُتنوعة من المُنتجات والخدمات أن تعمل بأنظمتها المالية في مواقع مُتعددة، وبدعم من مُختلف مُقدمي الخدمات.

وتواجه المؤسسات المالية أيضاً التحدي المُتمثل في مواكبة إحتياجات وتفضيلات المُستهلكين الذين يكتسبون مزيداً من الخبرة في مجال تكنولوجيا المعلومات والاتصالات نظراً إلى سُرعة وسهولة إستخدام

الإنترنت والأجهزة المحمولة للحصول على الخدمات المالية، وتقوم المؤسسات المالية بشكل مُتزايد بنشر المزيد من التقنية المتقدمة والأنظمة عبر الإنترنت، بما في ذلك الأنظمة المصرفية عبر الانترنت، والخدمات المصرفية عبر الهاتف المحمول، وأنظمة الدفع، ومنصات التداول عبر الإنترنت، وبوابات التأمين للوصول إلى زبائنها. وفي هذا الصدد، يجب أن تَتَفَهّم المؤسسات المالية بشكل كامل حجم وكثافة مخاطر التكنولوجيا من هذه الأنظمة. كما يجب أن تضع أنظمة إدارة المخاطر كافية وقوية، فضلاً عن عمليات تشغيل لإدارة مثل هذه المخاطر.

تُحَدّد المبادئ التوجيهية لإدارة المخاطر التكنولوجية (المبادئ التوجيهية) الواردة في COBIT و ISACA والمعيار الدولي ISO31000 مبادئ إدارة المخاطر وأفضل الممارسات لتوجيه المؤسسات المالية، فيما يلي:

1. إنشاء إطار قوي ومتين لإدارة مخاطر التقنية.
2. تعزيز أنظمة الحماية والموثوقية والمرونة والقابلية للإسترداد.
3. تطبيق عمليات توثيق مُحكمة لحماية بيانات الزبائن والعمليات والأنظمة.

إن درجة التقيّد بهذه المبادئ من قبل مؤسسة ما، سيُعتمد من قبل المصرف المركزي معياراً لتقييم مخاطر هذه المؤسسة.

ثانياً: نطاق وآلية التطبيق والأطراف المعنية:

على جميع المصارف وشركات الدفع الإلكتروني وفروع المصارف العاملة في ليبيا الإلتزام بهذه الضوابط بالقدر الذي ينطبق عليها، بِجانب إلتِزامِها بدليل وسياسات الحوكمة ذات الصلة، الصادرة عن مصرف ليبيا المركزي، وفي حال كانت المؤسسة سبق وأن إتَّبَعت تعليمات إحدى المؤسسات الدولية المُعترف بها، وترى المؤسسة أن إلتِزامِها السابق كان الأكثر تحقيقاً، فإن على المؤسسة تقديم ما يؤيد ذلك إلى المصرف المركزي، مع مُراعات عدم التعارض مع التشريعات المحلية، وفي حال وجود تعارض فعلى المؤسسة، إعلام إدارة الرقابة على المصارف والنقد بمصرف ليبيا المركزي بذلك، وتقديم التوضيح اللازم لهذا التعارض والحصول على موافقة مصرف ليبيا المركزي على أسلوب مُعالجة هذا التعارض، لتوحيد عمليات الرقابة والتدقيق.

وعلى المصارف عقد إتفاقية إسناد (Outsourcing) مع المصادر الخارجية لتوفير الموارد البشرية والخدمات والبُنى التحتية لتكنولوجيا المعلومات والاتصالات، بهدف تسيير عمليات المؤسسة، وعلى المصارف التأكد من إلتزام المصادر الخارجية بتطبيق بنود هذه الضوابط بشكل كلي أو جزئي بالقدر الذي يتناسب وأهمية

وطبيعة عمليات المؤسسة، والخدمات، والبرامج، والبنية التحتية المقدمة قبل وأثناء مدة التعاقد، وبما لا يعفي المجلس والإدارة التنفيذية من المسؤولية النهائية لتحقيق متطلبات الضوابط بما في ذلك متطلبات التدقيق الواردة في المادة (7)، وتُعد مدة نفاذ الضوابط أو مدة التعاقد المدة الزمنية الواجب خلالها توفيق أوضاع الشركة المتعاقد معها حالياً، ولا سيما أيهما أسبق.

يشمل نطاق تطبيق الضوابط كافة عمليات المؤسسة المُرتكزة على تكنولوجيا المعلومات والاتصالات بمختلف الفروع والإدارات، وتعد جميع الأطراف أصحاب المصلحة معنية بتطبيق الضوابط كل بحسب وظيفته وموقعه، ولتسهيل عملية التطبيق يتم البدء من خلال مشروع/ برنامج (مجموعة مشاريع ذات صلة) يُدار من قبل المؤسسة لإيجاد وتوفير البيئة اللازمة وتحقيق متطلبات هذه الضوابط، ونذكر على وجه التحديد الأطراف الآتية ومسؤولياتها الرئيسية بهذا الشأن:-

1. أعضاء المجلس والخبراء الخارجين المستعان بهم: تَوَلّي مسؤوليات التوجيه العام للمشروع/ البرنامج والموافقة على المهام والمسؤوليات ضمن المشروع، والدعم وتقديم التمويل اللازم.
2. المدير العام ونوابِهِ ومساعدوه، ومديرو العمليات والفروع: تولي مسؤوليات تسمية الأشخاص المناسبين من ذوي الخبرة بعمليات المؤسسة لتمثيلهم في المشروع وتوصيف مهامهم ومسؤولياتهم.
3. مدير ولجان تكنولوجيا المعلومات والاتصالات التوجيهية، ومديرو المشاريع: تولي مسؤوليات إدارة المشروع / البرنامج وتوجيهه والإشراف بشكل مباشر، والتوصية بتوفير المواد اللازمة لإتمامه، والتأكد من الفهم الصحيح من قبل الأطراف كافة بمتطلبات وأهداف الضوابط المحددة في هذا الدليل.
4. التدقيق الداخلي: تولي مسؤولياته المُناطة بِهِ 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.
5. على إدارات "المخاطر، وأمن المعلومات، والامتثال، والقانونية": تولي مسؤوليات المشاركة في المشروع/ البرنامج بما يمثل دور تلك الإدارات، والتأكد من تمثيل المشروع/ البرنامج من قبل الأطراف المعنية كافة.
6. المتخصصون وحملة الشهادات الفنية والمهنية الخاصة بأفضل الممارسات (COBIT Assessor, Implementation, COBIT Foundation, CGEIT) المستعان بهم من داخل المؤسسة ومن خارجها: تولي مهمة المُرشد لنشر المعرفة بالمعيار وتسهيل عملية التطبيق.

على المصارف تحديد إطار زمني وخطة عمل خلال ستة أشهر وفقاً لهذه الضوابط، على أن تتضمن هذه الخطة الموازنات اللاحقة التي تضمن تطبيق هذه الضوابط، والوصول إلى مُستوى نضوج (3.2) (Deployment Maturity level 3.2: Established) بعد 18 شهراً بحد أقصى من تاريخ هذه العمليات الأساسية المتعلقة بتكنولوجيا المعلومات، والوصول لمستوى نضوج (5.2) (Maturity level 5.2: Optimization) خلال 36 شهراً، حداً أقصى من تاريخها، وبشكل كامل جميع الأعمال المتعلقة بتكنولوجيا المعلومات، على أن تتم مُراجعة مُستوى النضوج للأعمال غير المتعلقة بتكنولوجيا المعلومات والاتصالات وفقا لخطة العمل التي إعتمدتها المؤسسة، والوصول إلى نضوج (5.2) لمدة لا تتجاوز خمس سنوات لجميع الأعمال المتعلقة وغير المتعلقة بتكنولوجيا المعلومات والاتصالات.

يعد تطبيق مُتطلبات التعليمات خطوة أولى ونقطة شروع وبداية باتجاه التطوير والتحسين المُستمرين لحوكمة المعلومات وإدارتها، والتكنولوجيا المصاحبة لها. وعليه، يتوجب على إدارات المصارف مواكبة الإصدارات الناشئة المستقبلية وتحديثاتها فيما يخص الإطار العام الذي تم الإستناد عليه عند صياغة هذه الضوابط (COBIT 19)، وما يحتويه من معايير دولية أخرى مُسانِدة له ضمن هذا الإطار.

ولا بد عند التطبيق والدخول في تفاصيلنا الركائز (الدعامات) السبعة، والعمليات، والأهداف الفرعية، أن تقوم المصارف بتطويع (Tailoring) كل ذلك بما ينسجم بمعطيات كل مصرف على حدى، في سبيل خدمة أهداف ومتطلبات الضوابط والمعيار (COBIT 19)، والعمل على إيجاد التغيير المطلوب لتوفير وتهيئة البيئة اللازمة للتطبيق.

وإتّباع أسلوب تحليل الإنحراف (Gab Analysis) بين الوضع الحالي، ومُقارنة مع مُتطلبات الضوابط والمعيار تمهيداً لعملية التطبيق.

وعلى المصارف أرسال تقارير الإيجاز المتعلقة بالامتثال لتحقيق متطلبات ضوابط مصرف ليبيا المركزي كل ستة أشهر من تاريخ الضوابط، موضحةً فيها مستوى الإيجاز لكل بند من بنود ضوابط للعمليات المتعلقة وغير المتعلقة بتكنولوجيا المعلومات.

ثالثاً: أهداف ضوابط حوكمة تكنولوجيا المعلومات والاتصالات في القطاع المصرفي الليبي:

تُعد الأهداف وعمليات دليل حوكمة تكنولوجيا المعلومات بحسب المرفقين (2) و (3)، ومعطياتها حد أدنى ويتوجب على إدارة المؤسسة الامتثال لها، وتحقيقها بشكل مستمر، وتُعَدُ اللجنة التوجيهية لتكنولوجيا المعلومات المسؤول الأول عن ضمان الامتثال بتحقيق مُتطلباتها، ولجنة حوكمة تكنولوجيا المعلومات

والمجلس بصورة كلية، هي المسؤول النهائي بهذا الشأن، ويتوجب على إدارات المؤسسة كافة، وبصورة خاصة إدارة تقنية المعلومات وإدارة أمن المعلومات و إدارة المشاريع تحديد عملياتها وإعادة صياغتها، بحيث تحاكي وتغطي متطلبات جميع عمليات وأهداف حوكمة وإدارة تكنولوجيا المعلومات الواردة في المُرفق (3).

يتولى المجلس للمسؤوليات المباشرة لعمليات التقييم والتوجيه والرقابة، فضلاً عن مسؤولياته المباشرة عن عملية ضمان إدارة رشيدة لمخاطر تكنولوجيا المعلومات وعملية إدارة المخاطر الواردة في المرفق رقم (3) على التوالي، بالتعاون مع إدارة المخاطر في المؤسسة، إذ تهدف هذه الضوابط إلى تلبية إحتياجات أصحاب المصالح (Stakeholder's Needs) وتحقيق توجهات وأهداف المؤسسة من خلال تحقيق أهداف تكنولوجيا المعلومات، بما يضمن:

1. توفير معلومات ذات جودة عالية تكون مرتكزاً يدعم آليات صنع القرار في المؤسسة.
2. إدارة رشيدة لموارد ومشاريع تكنولوجيا المعلومات للاستفادة من تلك الموارد، وتقليل الهدر فيها.
3. توفير بنية تحتية لتقنية متميزة وداعمة تُمكن المؤسسة من تحقيق أهداف الحوكمة.
4. الارتقاء بعمليات المؤسسة المُختلفة من خلال توظيف منظومة تقنية كفوءه وذات إعتمادية مُتميزة.
5. إدارة رشيدة لمخاطر تقنية المعلومات والاتصالات تكفل الحماية اللازمة لأصول المؤسسة.
6. المساعدة في تحقيق الامتثال لمتطلبات القوانين والتشريعات والضوابط، فضلاً عن الامتثال لإستراتيجية وسياسة وإجراءات العمل الداخلية.
7. تحسين نظام الرقابة الداخلي.
8. تحسين مستوى الرضى عن تقنية المعلومات والاتصالات من قبل مستخدميها بتلبية إحتياجات العمل بكفاءة وفاعلية.
9. إدارة خدمات الأطراف الخارجية الموكل إليها تنفيذ عمليات ومهام الخدمات والمنتجات المتعلقة بتقنية المعلومات.

تبني أفضل المعايير الدولية والممارسات وقواعد العمل والتنظيم، مثل: BASEL, ISO , COBIT [27000مكتبة البنية التحتية لتقنية المعلومات والإتصالات] (ISO 20000) (ITIL)، نقطة إنطلاق يتم الإرتكاز والبناء عليها في مجالي حوكمة وإدارة عمليات ومشاريع ومواد تكنولوجيا المعلومات والاتصالات.

فصل عمليات ومهام ومسؤوليات المجلس في مجال الحوكمة عن تلك التي تقع ضمن حدود ومسؤولية الإدارة التنفيذية بشأن المعلومات والتقنية ذات الصلة.

تعزيز آليات الرقابة الذاتية والرقابة المستقلة، وفحص الامتثال في مجالي حوكمة وإدارة المعلومات والتقنية ذات الصلة، وبما يسهم في تحسين وتطوير الأداء بشكل مُستمر.

رابعاً: نشر ضوابط حوكمة وإدارة المعلومات والتقنية ذات الصلة:

على كل مصرف نشر إجراءاته المُتخذة فيما يخص دليل حوكمة تكنولوجيا المعلومات والاتصالات، وبأي طريقة أخرى مُناسبة لإطلاع الجمهور، وعلى المؤسسة الإفصاح في تقريرها السنوي عن وجود دليل خاص لحوكمة وإدارة المعلومات وتكنولوجيا المصاحبة لها، أو مُتَضَمّناً لدليل الحوكمة المؤسسية لديه، وعلى مدى إلتزامِهِ بتطبيق ما جاء في هذا الدليل.

خامساً: اللّجان:

أ. لجنة حوكمة تكنولوجيا المعلومات:

على المجلس تشكيل لجنة حوكمة تكنولوجيا المعلومات، وتتشكل هذه اللجنة من ثلاثة أعضاء على الأقل، ويُفضل أن تضم في عضويتها أشخاص من ذوي الخبرة أو المعرفة الاستراتيجية في تقنية المعلومات والاتصالات، وللّجنة الاستعانة عند اللزوم على نفقة المؤسسة بخبراء خارجيين وذلك بالتنسيق مع رئيس المجلس، لغرض تعويض النقص في هذا المجال من جهة، ولتعزيز الرأي الموضوعي من جهة أخرى، وللّجنة دعوة أي من إداريي المؤسسة لحضور إجتماعاتها، للإستعانة برأيهم بما فيهم المعنيين بالتدقيق الداخلي وأعضاء الإدارة التنفيذية (مثل مدير تقنية المعلومات) أو المعنيين في التدقيق الخارجي، ويُحدد المجلس أهدافها و يفوضها بصلاحيات من قِبَله، بدأ ذلك وفق مثاق يوضح ذلك، على أن تقوم برفع تقارير دورية للمجلس، علماً بأن تفويض المجلس صلاحيات للجنة أو أي لجنة أخرى لا يعفيه بصورة كلية من تحمل مسؤولياته بهذا الشأن، وتجتمع اللجنة بشكل دوري (ثلاثة أشهر على الأقل)، وتحتفظ بمحاضر إجتماعات موثقة، وتتولى المهام الآتية:

1. إعتماد الخطط الاستراتيجية لتكنولوجيا المعلومات والاتصالات والهيكل التنظيمي المناسبة، بما في ذلك اللجان التوجيهية على مستوى الإدارة التنفيذية وبصورة خاصة (اللجنة التوجيهية لتقنية المعلومات والاتصالات)، وبما يضمن تحقيق الأهداف الاستراتيجية للمؤسسة وتلبيتها، وتحقيق أفضل القيم المُضافة من مشاريع وإستثمارات موارد تقنية المعلومات والاتصالات، واستخدام الأدوات والمعايير اللازمة لمراقبة والتأكد من مدى تحقيق ذلك، مثل استخدام نظام بطاقات الأداء

المتوازنة لتقنية المعلومات والاتصالات (IT Balanced Scorecards) و إحتساب معدل العائد على الاستثمار (ROI)، وقياس أثر المُساهمة في زيادة الكفاءة المالية والتشغيلية.

2. إعتماد الإطار العام لإدارة وضبط ومُراقبة موارد ومشاريع تقنية المعلومات والاتصالات، يحاكي أفضل المؤسسات الدولية المقبولة بهذا الشأن، وعلى وجه التحديد (COBIT) Control Objective for Information and Related Technology بجميع الإصدارات هذه تحقيق أهداف ومتطلبات هذه الضوابط من خلال تحقيق الأهداف المؤسسية، الواردة في المرفق رقم (1) بشكل مستدام، وتحقيق مصفوفة أهداف المعلومات والتكنولوجيا المصاحبة لها، الواردة في المرفق رقم (2)، ويغطي عمليات حوكمة تكنولوجيا المعلومات والاتصالات الواردة في المرفق رقم (3).
3. إعتماد مصفوفة الأهداف المؤسسية، الواردة في المرفق رقم (1)، وأهداف المعلومات والتقنية ذات الصلة، الواردة في المرفق رقم (2)، وعد معطياتها حداً أدنى، وتوصيف الأهداف الفرعية لتحقيقها.
4. إعتماد مصفوفة للمسؤوليات (RACI Chart) إتجاه العمليات الرئيسية لحوكمة تكنولوجيا المعلومات والاتصالات في المرفق رقم (3)، والعمليات الفرعية المنبثقة عنها من حيث: الجهة أو الجهات أو الشخص أو الأطراف المسؤولة بشكل أوّلي Responsible، وتلك المسؤولية بشكل نهائي Accountable، والأطراف الاستشارية Consultant، وتلك التي يتم إطلاعها تجاه كل العمليات Informed في المرفق المذكور بهذا الشأن.
5. التأكد من وجود إطار عام لإدارة مخاطر تقنية المعلومات والاتصالات يتوافق والإطار العام الكلي لإدارة المخاطر في المؤسسة ويتكامل معه، وفقاً للمعايير الدولية مثل (ISO 31000, ISO 73) ويأخذ بالحسبان جميع عمليات حوكمة تكنولوجيا المعلومات والاتصالات الواردة في المرفق رقم (3)، ويلبيها.
6. إعتماد موازنة موارد ومشاريع تقنية المعلومات والاتصالات بما يتوافق والأهداف الاستراتيجية للمؤسسة.
7. الإشراف العام والإطلاع على سير عمليات وموارد ومشاريع تقنية المعلومات والاتصالات للتأكد من كفايتها ومساهمتها الفاعلة في تحقيق متطلبات المؤسسة وأعمالها.
8. الاطلاع على تقارير التدقيق لتقنية المعلومات والاتصالات، واتخاذ ما يلزم من إجراءات لمعالجة الانحرافات ورفع التوصيات باتخاذ الإجراءات اللازمة لتصحيحها.

مُلاحظة: تُدمج مهام لجنة حوكمة تكنولوجيا المعلومات مع مهام لجنة حوكمة المصارف مرحلةً أولى لمدة سنة – ثلاث سنوات بعد ذلك تنفصل اللجنة وتُصبح لجنة حوكمة تكنولوجيا المعلومات مُنفصلة عن لجنة حوكمة المصارف.

ب. اللجنة التوجيهية لتكنولوجيا المعلومات.

على الإدارة التنفيذية تشكيل اللجنة التوجيهية لتكنولوجيا المعلومات والاتصالات لتحقيق الأهداف الاستراتيجية للمؤسسة وبشكل مُستدام، وعليه يتم تشكيل لجنة تسمى باللجنة التوجيهية لتكنولوجيا المعلومات، برئاسة المدير العام والمُدراء الفرعيين، بما في ذلك مدير لتقنية المعلومات ومدير إدارة المخاطر ومدير أمن المعلومات، وينتخب المجلس أحد أعضائه ليكون عضواً مراقباً بهذه اللجنة، فضلاً عن مدير التدقيق الداخلي الذي تكون مهمته مراقباً، وليس عضواً في اللجنة، ويتم حضوره فقط عند تقديم أو مناقشة تقريره لتحقيق مبدأ الشفافية والموضوعية، ويمكنها دعوة الغير لدى الحاجة لحضور اجتماعاتها، وتوثق اللجنة اجتماعاتها بمحاضر، وتجتمع اللجنة التوجيهية دورياً مرة كل ربع سنة على الأقل، وتتولى بصورة خاصة القيام بالمهام الآتية:

1. وضع الخُطط السنوية الإستراتيجية والتشغيلية لإدارة المخاطر الكفيلة بالوصول إلى الأهداف الاستراتيجية المقررة من قبل المجلس، والإشراف على تنفيذها لضمان تحقيقها لمراقبة العوامل الداخلية والخارجية المؤثرة فيها بشكل مُستمر.
2. ربط مصفوفة الأهداف المؤسسية بمصفوفة أهداف المعلومات والتكنولوجيا ذات الصلة، كما وردت في المرفق رقم (2)، واعتمادها ومراجعتها بشكل مستمر، وبما يضمن تحقيق الأهداف الاستراتيجية للمؤسسة وأهداف الضوابط، ومراعاة تعريف مجموعة معايير للقياس ومراجعتها وتكليف المعنيين من الإدارة التنفيذية بمراقبتها بشكل مستمر وإطلاع اللجنة على ذلك.
3. التوصية بتخصيص الموارد المالية وغير المالية اللازمة لتحقيق الأهداف وعمليات حوكمة تكنولوجيا المعلومات، الواردة في المرفقين (2) و (3) على التوالي، حداً أدنى، والاستعانة بالعنصر البشري الكفوء والمناسب في المكان المناسب، من خلال هياكل تنظيمية تشمل كل العمليات اللازمة لدعم الأهداف التي تراعي فصل المهام، وعدم تضارب المصالح وتطوير البنية التحتية التقنية والخدمات الأخرى المتعلقة بها خدمة للأهداف، وتولى عمليات الإشراف على سير تنفيذ مشاريع حوكمة تكنولوجيا المعلومات وعملياتها.
4. ترتيب مشاريع وبرامج تكنولوجيا المعلومات بحسب الأولوية.
5. مُراقبة مُستوى الخدمات الفنية والتقنية والعمل على رفع كفاءتها وتحسينها بشكل مستمر.
6. رفع التوصيات اللازمة للجنة حوكمة تكنولوجيا المعلومات بشأن الأمور الآتية:
   - تخصيص الموارد اللازمة والآليات الكفيلة بتحقيق مهام لجنة حوكمة تكنولوجيا المعلومات.
   - أية إنحرافات قد تؤثر سلباً في تحقيق الأهداف الاستراتيجية.

- أية مخاطر غير مقبولة متعلقة بتكنولوجيا المعلومات وأمنها وحمايتها.
- تقارير الأداء والإمتثال بمتطلبات الإطار العام لإدارة وضبط ومراقبة موارد ومشاريع تكنولوجيا المعلومات.

7. تزويد لجنة حوكمة تكنولوجيا المعلومات بمحاضر اجتماعاتها أولاً بأول، والحصول على ما يُفيد للاطلاع عليها.

سادساً: التدقيق الداخلي والخارجي:

مع زيادة تعقيد مخاطر تكنولوجيا المعلومات هناك حاجة مُتزايدة لتطوير منظومة رقابة داخلية فعالة لإدارة مخاطر التكنولوجيا.

توفر عمليات التدقيق في تكنولوجيا المعلومات لمجلس الإدارة والإدارة العليا تقييماً مُستقلاً وموضوعياً لإدارة المخاطر التقنية.

ويجب على المؤسسة إنشاء هيكل تنظيمي وتقارير لعمليات التدقيق في تقنية المعلومات والاتصالات بطريقة تحافظ على استقلالية وموضوعية عمليات التدقيق في تكنولوجيا المعلومات.

أ- على المجلس رصد الموازنات الكافية وتخصيص الأدوات والموارد اللازمة، بما في ذلك العنصر البشري المؤهل من خلال أقسام متخصصة بالتدقيق على تقنية المعلومات والاتصالات، والتأكيد أن كل من إدارة التدقيق الداخلي في المؤسسة والمدقق الخارجي قادران على مراجعة عمليات توظيف مواد ومشاريع التقنية في المعلومات والاتصالات وإدارتها وعمليات المؤسسة المرتكزة عليها، نمراجعة فنية متخصصة (IT Audit)، وتدقيقها، بحسب البند (ث) من هذه المادة، من خلال كوادر مهنية مؤهلة ومعتمدة دولياً في هذا المجال، حاصلين على شهادات اعتماد مهنية سارية مثل (CISA)، من مؤسسات دولية مؤهلة بموجب معايير الاعتماد الدولي للمؤسسات المانحة للشهادات المهنية (ISO / IEC 17024) و/أو أي معايير أخرى موازية.

ب- على لجنة التدقيق المنبثقة عن المجلس من جهة، والمدقق الخارجي من جهة أخرى، تزويد مصرف ليبيا المركزي بتقرير سنوي للتدقيق الداخلي، وآخر للتدقيق الخارجي على التوالي، يتضمن رد الإدارة التنفيذية واطلاع وتوصيات المجلس بشأنه، وذلك بحسب ما ورد في البند (ث/2) من هذه المادة وفقاً لنموذج تقرير تدقيق (مخاطر – ضوابط) المعلومات والتكنولجيا ذات الصلة، في

المرفق رقم (4)، وذلك خلال الربع الأول من كل عام، وتحل هذه التقارير محل نظيرتها أو التي تشملها من التقارير المطلوبة بموجب ضوابط سابقة.

ت- على لجنة التدقيق تضمين مسؤوليات عمل تدقيق تقنية المعلومات والاتصالات وصلاحياتها، ونطاقه، ضمن ميثاق التدقيق (Audit Charter) من جهة، ضمن إجراءات متفق عليها مع المدقق الخارجي من جهة أخرى، وبما يتفق مع هذه الضوابط ويغطيها.

ث- على المجلس التأكد من خلال لجنة التدقيق المنبثقة عنه، من التزام المدقق الداخلي والمدقق الخارجي للمؤسسة، لدى تنفيذ عمليات تدقيق المختص بالمعلومات والتقنية ذات الصلة، بما يأتي:

1- معايير تدقيق تقنية المعلومات والاتصالات بحسب آخر تحديث للمعيار الدولي Information Technology Assurance Framework (I'TAf) الصادر عن جمعية التدقيق والرقابة على نظم المعلومات (ISACA) ومنها:

- تنفيذ مهام التدقيق ضمن الخطة المعتمدة بهذا الشأن تأخذ في الحسبان الأهمية النسبية للعمليات ومستوى المخاطر ودرجة التأثير في أهداف ومصالح المؤسسة.
- توفير الإلتزام بخطط التدريب والتعليم المستمر من قبل الكادر المتخصص في هذا الصدد.
- الالتزام بمعايير الاستقلالية المهنية والإدارية وضمان عدم تضارب المصالح الحالية والمُستقبلية.
- الالتزام بالمعايير الموضوعية وبذل العناية المهنية والحفاظ المستمر على مستوى التنافسية والمهنية من المعارف والمهارات الواجب التمتع بها، ومعرفة عميقة بآليات وعمليات المؤسسة المختلفة المرتكزة على تقنية المعلومات والاتصالات وتقارير المراجعة والتدقيق الأخرى (المالية والتشغيلية والقانونية)، والقدرة على تقييم الدليل المتناسب مع الحالة والوضع العام في كشف الممارسات غير المقبولة والمخالفة لأحكام القوانين والأنظمة والضوابط.

2- فحص عملية توظيف وإدارة مواد تقنية المعلومات والاتصالات، وتقييمها ومراجعتها، وكذلك عمليات المؤسسة المرتكزة عليها، وإبداء رأي عام (Reasonable overall Audit Assurance) حيال مستوى المخاطر الكلي للمعلومات والتقنية ذات الصلة ضمن برنامج تدقيق يشمل على الأقل المحاور المبينة في المرفق رقم (5) على أن يكون تكرار التدقيق للمحاور كافة أو جزء منها، حد الأدنى مرة واحدة سنوياً على الأقل في حالة تم تقييم المخاطر بدرجة (4 أو 5) بحسب سُلّم

تقييم المخاطر الموضح في المرفق رقم (4)، ومرة واحدة كل سنتين على الأقل في حالة تم تقييم المخاطر بدرجة (3)، ومرة واحدة كل ثلاث سنوات على الأقل في حالة تم تقييم المخاطر بدرجة (2 او 1)، مع مراعاة التغير المستمر في مستوى المخاطر والأخذ بالحسبان التغيرات الجوهرية التي تطرأ على بيئة المعلومات والتقنية ذات الصلة خلال مدة تدقيق المذكورة، على أن يتم تزويدها بتقارير التدقيق لأول مرة بغض النظر عن درجة تقييم المخاطر، وعلى أن تشمل عمليات التقييم للمحاور المذكورة في آليات المؤسسة المتبعة، من حيث التخطيط الاستراتيجي ورسم السياسات، والمبادئ وإجراءات العمل المكتوبة والمعتمدة، وآليات توظيف الموارد المختلفة، بما فيها مواد تقنية المعلومات والاتصالات والعنصر البشري، وآليات وأدوات المُراقبة والتحسين والتطوير، والأعمال على توثيق نتائج التدقيق وتقييمُها إستناداً إلى أهمية الاختلافات و نقط الضعف (المُلاحظة)، فضلاً عن الضوابط المفعلة وتقييم مستوى المخاطر المتبقية والمتعلقة بكل منها باستخدام معيار منهجي لتحديد وقياس المخاطر، متضمناً الإجراءات التصحيحية المتفق عليها، والمنوي إتباعها من قبل إدارة المؤسسة، بتواريخ محددة للتصحيح، مع الإشارة ضمن جدول خاص يُعتمد من المسؤول في المؤسسة عن مُلاحظاته.

3- إجراءات منتظمة لمتابعة نتائج التدقيق للتأكد من معالجة المُلاحظات والاختلافات الواردة في تقارير المدقق بالمواعيد المُحددة، والعمل على رفع مستوى الأهمية والمخاطر تصعيداً تدريجياً في حالة عدم الاستجابة، وإعلام المجلس بذلك كلما تطلب الأمر.

4- تضمين آليات التقييم السنوي (Performance Evaluation) لكوادر تدقيق تقنية المعلومات والاتصالات بمعايير قياس موضوعية، على أن تتم عمليات التقييم من قبل المجلس مُمثلاً بلجنة التدقيق المنبثقة عنه، وبحسب التسلسل الإداري التنظيمي لإدارة التدقيق، أو من يحل محلها.

هـ- من المُمكن إسناد مهمة المدقق الداخلي للمعلومات والتقنية ذات الصلة (Internal IT Audit) إلى جهة خارجية مختصة مُستقلة تماماً عن المدقق الخارجي المعتمد بهذا الشأن (Outsourcing)، شريطة تلبية جميع متطلبات هذه الضوابط، وأي ضوابط أخرى ذات صلة، واحتفاظ لجنة التدقيق المنبثقة عن المجلس، والمجلس نفسه بوظيفتهما، فيما يتعلق بفحص الامتثال والتأكد من تلبية هذه المتطلبات، حداً أدنى.

سابعاً: الإطار العام لإدارة مخاطر تكنولوجيا المعلومات:

تشكل لجنة لإدارة المخاطر المنبثقة عن مجلس إدارة المؤسسة بحسب دليل الحوكمة المؤسسية الصادرة عن مصرف ليبيا المركزي مهامها وضع إستراتيجية، وإدارة الأدوار والمسؤوليات في عملية إدارة المخاطر، وتوزيعها، إلى جانب وجود إدارة المخاطر في كل مؤسسة تتولى جميع مهام وفاعليات إدارة المخاطر لتكنولوجيا المعلومات، وتتشكل هذه اللجنة من ثلاثة أعضاء في الأقل من الأعضاء غير التنفيذيين على أن يكون رئيس اللجنة عضواً مُستقلاً، ويجب أن يمتلك أعضاء اللجنة الخبرة أو المعرفة في إدارة المخاطر والمُمارسات والقضايا المرتبطة بتقنية المعلومات والاتصالات، وينبغي إنشاء إطار لمفاهيم إدارة مخاطر تقنية المعلومات والاتصالات بطريقة منتظمة ومنسقة. وأن يشمل الصفات الآتية:

1. القواعد والمسؤوليات.
2. تحديد وترتيب أولويات أصول نظام المعلومات.
3. تحديد وتقييم التهديدات والمخاطر المحتملة ونقاط الضعف الحالية والناشئة.
4. تطبيق المعايير الدولية (ISO: 31000 GXM) NIST, COBIT for IT, ISO/IEC 27005:2018, RISK,.
5. تطبيق المُمارسات والرقابة المناسبة للتخفيف من المخاطر.
6. تحديث دوري وتقييم للمخاطر بما يشمل التغييرات في النظم البيئية أو الظروف التشغيلية التي قد تؤثر على تحليل المخاطر.

ينبغي وضع مُمارسات فعالة لإدارة المخاطر والرقابة الداخلية لتحقيق سرية البيانات، وأمن النظام، والموثوقية، والمرونة، والقابلية للتعافي في المؤسسة.

حماية أصول أنظمة تكنولوجيا المعلومات والاتصالات:

الحماية الكافية والمناسبة لأصول النظام من الوصول غير المخول وسوء الاستخدام والإحتيال و الإدراج والحذف والاستبدال والكشف والإلغاء، يجب على المؤسسة وضع سياسات واضحة لحماية أصول النظام وتحديد أهميته والتحقق من صحته من أجل وضع خطط مناسبة لحمايته.

عملية إدارة المخاطر:

المخاطر هي دالة على إحتمال وجود مصادر تهديد معينة نتيجة نقط ضعف مُحتملة يترتب عليها أثر سلبي في المؤسسة بشكل عام، ولتحديد إحتمال وقوع حدث سلبي مُستقبلي ،يجب تحليل التحديات التي تعرض

لها نظم تقنية المعلومات، بالإقتران مع نقط الضعف المُحتملة والضوابط المعمول بها، إذ تتضمن عملية إدارة المخاطر البدء بتحليل بيئة الخطر، وتحديد المخاطر، وتحليلها، وتقييمها، ومعالجتها، من خلال عملية مستمرة وفقاً لمعيار ISO:31000 المعتمدة، على النحو التالي:

1-تحليل بيئة تكنولوجيا المعلومات:

يتطلب تحديد المخاطر لتقنية المعلومات الفهم الدقيق لبيئة النظم؛ لذلك يجب جمع المعلومات المتعلقة بتقنية المعلومات، والتي عادة ما تصنف على النحو الآتي:

أجهزة ملموسة.

البرامجيات.

البيانات والمعلومات.

الأشخاص الذين يدعمون ويستخدمون تقنية المعلومات.

مهمة النظام.

مستوى حرجية النظام والبيانات، على سبيل المثال قيمة النظام أو أهميته للمؤسسة. حساسية النظام والبيانات، ومستوى الحماية المطلوبة للحفاظ على النظام وسلامة البيانات، والسرية وتوافرها.

2- تقدير المخاطر:

أ- تحديد المخاطر

- **التعرف على التهديدات**

يجب تحديد التهديدات وأوجه الضعف في بيئة تكنولوجيا المعلومات والاتصالات للمؤسسات المالية، التي تشمل الشبكات الداخلية والخارجية، والأجهزة والبرامج والتطبيقات المرتبطة بالأنظمة والعمليات، والعناصر البشرية.

قد تكون التهديدات على شكل عوامل أو حالات أو حوادث أو أشخاص مع احتمال أن يتسبب في أضرار من خلال استغلال الضعف في النظام. ويمكن أن يكون مصدر التهديد من العوامل الطبيعية أو العوامل البشرية أو العوامل البيئية. وتعد العوامل البشرية من أهم مصادر التهديدات من خلال الأخطاء المتعمدة أو غير المتعمدة التي يمكن أن تلحق ضرراً شديداً بالمؤسسة ونظم المعلومات الخاصة بها عند إدارتها من قبل أشخاص غير أكفاء.

التهديدات الأمنية كتلك التي تتجلى في هجمات المنع من الخدمة والتخريب الداخلي، وهجمات البرمجيات الخبيثة، يمكن أن تتسبب في ضرر شديد، وتعطيل لعمليات المؤسسة، والخسائر اللاحقة لجميع الأطراف المُتضررة ويجب أن تكون المؤسسة يقظة في مراقبة مثل هذا النوع من المخاطر المتغيرة والمتنامية؛ لأنها خطوة مُهمة في ممارسة إحتواء هذه المخاطر.

- **التعرف على قابلية التعرض للتهديدات**

يجب أن يتضمن تحليل التهديدات لتقنية المعلومات تحليلاً لنقاط الضعف المرتبطة مع بيئة النظام، والهدف هو التعرف على (العيوب أو نقاط الضعف) التي يمكن إستغلالها من مصادر التهديد المُحتملة.

ب تقييم المخاطر

- **تحديد الاحتمالية**

لتحديد احتمالية إمكانية التعرض لتهديد مُحتمل لأنظمة تقنية المعلومات يجب مُراعاة العوامل الآتية:

- الدافع لمصدر التهديد ومقدرة ذلك المصدر .
- طبيعة الضعف.
- وجود الضوابط الرقابية الحالية وفاعليتها.

ويمكن وصف احتمالية تعرض الثغرات المحتملة لمصدر تهديد معين بأنها عالية، أو متوسطة، أو منخفضة.

- **تحليل الأثر**

هي عملية تحديد الأثر السلبي الناشئ عن تحقق تهديد ناجح لثغرات، أو نقط الضعف في نظم تقنية المعلومات، وقبل البدء بعملية تحليل الأثر من الضروري الحصول على المعلومات الآتية:

- مهمة النظام.
- أهمية النظام والبيانات.
- حساسية النظام والبيانات.

- **تحديد مُستوى المخاطر**

تحديد مستوى المخاطر التي تتعرض لها نظم تقنية المعلومات، ويمكن التعبير عنه دالة لـ::

- إحتمال وجود مصدر تهديد أو خطر معين نتيجة نقطة ضعف معينة.
- مُستوى التأثير الناتج عن الثغرات الأمنية، في النظام وممارسة مصدر التهديد بنجاح.
- مدى كفاية الضوابط الأمنية المخطط لها، أو القائمة، لتقليل المخاطر أو القضاء عليها.

ج - مُعالجة المخاطر:

- لكل نوع من أنواع المخاطر يجب تنفيذ إستراتيجيات التخفيف والرقابة التي تتفق مع أصول النظام ومستوى تحمل المخاطر.
- يستلزم تخفيف المخاطر واتباع نموذج منهجي لتقييم وتحديد أولويات الضوابط المناسبة للحد من المخاطر. ومجموعة من الضوابط الفنية والإجرائية والتشغيلية والوظيفية التي من شأنها توفير طريقة فعالة لتقليل المخاطر.
- قد لا يكون من العملي مُعالجة جميع المخاطر المكتشفة في الوقت نفسه، أو في الإطار الزمني نفسه، يجب أن تعطي المؤسسة الأولوية للتهديدات التي تحتوي على نسب مخاطرة عالية، والتي يمكن أن تسبب ضرراً كبيراً على عمليات المؤسسة ويجب على المؤسسة تقييم قدرتها على تحفل المخاطر والأضرار والخسائر في حالة وقوع حدث معين وينبغي أيضاً أن تكون هناك موازنة بين تكاليف الرقابة على المخاطر وبين الفوائد المُتأتية منها.
- من الضروري أن تكون المؤسسة قادرة على إدارة المخاطر ومُراقبتها بطريقة تحافظ بها على سلامة واستقرار الوضع المالي والتشغيلي. وعند تبني الرقابة البديلة وتدابير أمنية جديدة يجب على المؤسسة أن تكون مُدركة لتكاليف وفاعلية الرقابة المتعلقة بالمخاطر التي يتم تخفيفُها.
- يجب على المؤسسة عدم تطبيق أو تشغيل أي نظام ضعيف، أو لا يمكن فيه مواجهة مخاطر النظام ومراقبتها بشكل كافٍ.
- بصفة إجراء مُخفف للمخاطر يمكن للمؤسسة الحصول على بوليصة تأمين لتغطية مختلف المخاطر القابلة للتأمين بما في ذلك تكاليف الإصلاح والتعويض.

رصد المخاطروإعداد التقارير:

- يجب أن تحتفظ المؤسسة بسجل للمخاطر مما يُسهل عملية الرقابة على المخاطر والإبلاغ عنها. وينبغي إعطاء الأولوية القصوى للمخاطر الشديدة ورصدها عن كتب، مع الإبلاغ المنتظم عن الإجراءات التي اتخذت التخفيف منها. كما ينبغي للمؤسسة أن تقوم بتحديث سجلات المخاطر بشكل دوري، وأن تتم عمليات الرقابة والمراجعة لتقييم المخاطر ومعالجتها بشكل مستمر.
- لتسهيل إعداد تقارير المخاطر للإدارة يجب على المؤسسة تطوير وحدات قياس لمخاطر التقنية بحسب الأنظمة أو العمليات والبنية التحتية التي لديها أعلى نسب تعرض للمخاطر. كما يجب أيضاً توفير ملف كامل لمخاطر التقنية في المؤسسة إلى مجلس الإدارة والإدارة العليا وعند تحديد وحدات قياس المخاطر يجب على المؤسسة النظر في حدوث المخاطر والمتطلبات التنظيمية وملاحظات التدقيق.

- قد تتغير عوامل قياس المخاطر مع تغير بيئة تكنولوجيا المعلومات والاتصالات وقنوات التوزيع ومن ثم يجب على المؤسسة مراجعة وتحديث عمليات إدارة المخاطر وفقاً لذلك، وإجراء إعادة تقييم لأساليب مراقبة المخاطر السابقة مع أختبار مُتجدد، وتقييم مدى كفاية وفعالية عمليات إدارة المخاطر.
- يجب أن تقوم إدارة التقنية بمراجعة وتحديث نهج التحكم في مخاطر تقنية المعلومات والاتصالات والتخفيف منه، مع مراعاة الظروف المتغيرة والتغيرات في المخاطر المتعلقة بالمؤسسة.

الإشراف على مخاطر تكنولوجيا المعلومات والاتصالات من قبل مجلس الإدارة والإدارة العليا:

- تُعد تكنولوجيا المعلومات والاتصالات الوظيفة الأساسية للكثير من المؤسسات المصرفية. فعندما تفشل الأنظمة الحساسة ولا يستطيع الزبائن الوصول إلى حساباتهم المصرفية، قد تصبح العمليات المصرفية في حالة ركود، إذ سوف يكون التأثير فورياً في الزبائن مع وجود عواقب وخيمة على المؤسسات المصرفية، ومن هذه الأضرار، الأضرار الناجمة عن السمعة والمخالفات التنظيمية وخسائر الإيرادات والخسائر التجارية.
- ونظرًا إلى أهمية تكنولوجيا المعلومات والاتصالات في دعم أعمال المؤسسات المصرفية، يجب على مجلس الإدارة والإدارة العليا، الإشراف على مخاطر التقنية والتأكد من أن وظائف تقنية المعلومات والاتصالات في المؤسسة قادرة على دعم استراتيجيات وأهداف أعمالها.

(1) القواعد والمسؤوليات:

- يجب على مجلس الإدارة والإدارة العليا إنشاء إطار قوي ومتين لإدارة مخاطر التقنية. ويجب أيضا أن تتم مشاركة القرارات الاستراتيجية والمهمة لتقنية المعلومات والاتصالات فيما بينهم.
- يجب على مجلس الإدارة أن يكون مسؤولاً بشكل كامل عن فاعلية الرقابة الداخلية وممارسات إدارة المخاطر لتحقيق الأمن والموثوقية والمرونة وقابلية التعافي.
- يجب الأخذ بالحسبان قضايا التكاليف والفوائد، بما في ذلك عوامل مثل السمعة وثقة الزبائن والأثر المترتب عليها، والآثار القانونية المتعلقة بالاستثمار في عمليات الرقابة وإجراءات الحماية الخاصة لكل من أنظمة الحاسوب والشبكات ومراكز البيانات (DC) و عمليات وتسهيلات النسخ الاحتياطي.

(2) سياسات تكنولوجيا المعلومات والاتصالات والمعايير والإجراءات:

- يجب على المؤسسات المصرفية وضع السياسات والمعايير الخاصة بتكنولوجيا المعلومات والاتصالات، والتي تُعد من المكونات الأساس لإطار إدارة مخاطر التقنية وحماية أصول النظام في المؤسسة.
- بسبب التغيرات السريعة في عمليات تكنولوجيا المعلومات والاتصالات وبيئة الحماية تجب مراجعة السياسات والمعايير بشكل منتظم وتحديثها باستمرار.
- يجب تنفيذ عمليات الامتثال للتحقق من تطبيق معايير وإجراءات أمن تقنية المعلومات والاتصالات وينبغي تنفيذ عمليات المتابعة بحيث يتم معالجة الانحرافات عن الامتثال ومعالجتها في الوقت المناسب.

(3) عمليات اختيار الأشخاص:

- الاختيار الدقيق للموظفين والمزودين والمتعاقدين، أمر بالغ الأهمية؛ لتقليل مخاطر التقنية المتمثلة في فشل النظام والتخريب الداخلي والاحتيال وبما أن الأشخاص يلعبون دورا مهما في إدارة الأنظمة والعمليات المتعلقة ببيئة تكنولوجيا المعلومات والاتصالات، المعلومات فيجب على المؤسسات المصرفية تنفيذ عمليات فحص شاملة وفعالة.
- ينبغي أيضاً أن يُطلب من الموظفين والمزودين والمتعاقدين المخولين بالوصول إلى الأنظمة في المؤسسات المصرفية حماية المعلومات الحماسة والسرية.

(4) وعي أمن تقنية المعلومات والاتصالات:

- يجب إنشاء برنامج تدريبي شامل من أجل وعي أمن تقنية المعلومات والاتصالات لتعزيز مستوى الوعي في المؤسسة، وينبغي أيضاً أن يتضمن البرنامج التدريبي معلومات عن سياسات ومعايير أمن تقنية المعلومات والاتصالات، فضلا عن المسؤوليات الفردية والتدابير التي يجب اتخاذها لحماية أصول النظام. كما يجب أن يكون كل موظف في المؤسسة على دراية بالقوانين واللوائح والمبادئ التوجيهية المعمول بها ونشرها والوصول إليها.
- ينبغي إجراء برنامج التدريب وتحديثه في الأقل بشكل سنوي، وتوسيعه ليشمل جميع الموظفين الجدد والحالبين والمتعاقدين والمزودين الذين يستطيعون الوصول إلى موارد وأنظمة تقنية المعلومات والاتصالات في المؤسسة.
- ينبغي اعتماد برنامج التدريب من قبل الإدارة العليا. وينبغي مراجعته وتحديثه باستمرار للتأكد من أن محتويات البرنامج محدثة ومناسبة، وأن تأخذ المراجعة بالحسبان البيئة المتطورة للتقنية، فضلاً عن المخاطر الناشئة.

إدارة مخاطر الإسناد إلى مصادر خارجية (Outsourcing) لتكنولوجيا المعلومات والاتصالات:

الإسناد إلى مصادر خارجية (outsourcing) نأتي في كثير من الأشكال. بعض الأنواع الأكثر شيوعاً في الإسناد إلى مصادر خارجية (outsourcing) لتكنولوجيا المعلومات والاتصالات هي تطوير الأنظمة وصيانتها ودعم عمليات مركز البيانات وإدارة الشبكات وخدمات التعافي بعد الكوارث، وإضافة التطبيقات والحوسبة السحابية. وقد تنطوي عمليات الإسناد إلى مصادر خارجية (outsourcing) على توفير إمكانات وتسهيلات عمليات التقنية من قبل طرف ثالث أو موردين مُتعددين موجودين في ليبيا أو في الخارج.

الإجراءات لإرضاء المُتطلبات:

- ينبغي على مجلس الإدارة والإدارة العليا فهم المخاطر الكاملة المرتبطة بالإسناد إلى مصادر خارجية (outsourcing) لتكنولوجيا المعلومات والاتصالات قبل تعيين المزودين، والإجراءات لإرضاء المتطلبات يجب القيام بها لتحديد مدى قدرتها على البقاء والكفاءة والموثوقية وسجل التتبع والمركز المالي.
- ينبغي للمؤسسة أن يضمن الشروط التعاقدية والشروط التي تحكم المهام والعلاقات والالتزامات والمسؤوليات لجميع الأطراف المُتعاقدة بشكل كامل في إتفاقيات خطية، وعادة ما تشمل المتطلبات والشروط التي تغطى في الاتفاقيات.

وأهداف الأداء، ومُستويات الخدمة، والتوافرية والموثوقية، والقابلية للتطوير، والامتثال والتدقيق، والأمن، وتخطيط الطوارئ، وقدرة التعافي من الكوارث، وتسهيل معالجة النسخ الاحتياطية.

- يجب على المؤسسة التأكد من أن مزود الخدمات يمنح حق الوصول إلى جميع الأجزاء التي رشحتها المؤسسة للأنظمة والعمليات والوثائق الخاصة بها من أجل إجراء أية مراجعة أو تقييم لأغراض التنظيم أو التدقيق أو الامتثال.
- لا ينبغي أن تؤدي عمليات الإسناد إلى مصادر خارجية (outsourcing) إلى إضعاف وتدهور الرقابة الداخلية للمؤسسة. يجب على المؤسسة أن يطلب من مزود الخدمة توظيف مستوى عال من العناية والإجتهاد في السياسات الأمنية والإجراءات والرقابة لحماية سرية المعلومات وأمنها مثل بيانات الزبائن وملفات الحواسيب والسجلات والبرامج، وكود المصدر(Source Code).
- يجب على المؤسسة ومزود الخدمة الخارجي External Service Provider توقيع اتفاقية المحافظة على سرية المعلومات والبيانات (Non-Disclosure Agreement(NDA، فضلاً عن إتفاقية عدم تعيين موظفي المؤسسة لدى مزود الخدمة؛ لما في ذلك من خطورة على سرية البيانات والإجراءات في المؤسسة، واعتماد المعايير الدولية عند صياغة هذه الاتفاقيات.

- يجب على المؤسسة أن تطلب من مزود الخدمة تنفيذ السياسات الأمنية وإجراءات الرقابة ويجب أن تكون الإجراءات محكمة كما يطبقها المزود للنشاطات الخاصة به.
- يجب على المؤسسة مراقبة ومراجعة السياسات الأمنية وإجراءات الرقابة لمزود الخدمة على أساس منتظم، بما في ذلك الحصول على تقارير دورية عن مدى كفاية نشاطات الحماية والالتزام فيما يتعلق بالعمليات والخدمات التي يقدمها مزود الخدمة.
- يجب على المؤسسة أن تطلب من مزودي الخدمة تطوير وإنشاء إطار للتعافي من الكوارث الطارئة، ويجب أن يتم تحديد المهام والمسؤوليات في توثيق وحماية واختبار خطط الطوارئ والتعافي من الكوارث.
- يجب أن تتلقى جميع الأطراف المعنية بما في ذلك مقدمي الخدمات، تدريبا منتظما على تفعيل خطة الطوارئ وتنفيذ إجراءات التعافي.
- يجب مراجعة خطة التعافي من الكوارث وتحديثها واختبارها بانتظام وفقا للظروف المتغيرة والمتطلبات التشغيلية.
- يجب على المؤسسة أيضاً وضع خطة طوارئ تستند إلى أسوء سيناريوهات تعطل الخدمة؛ للتحضير لاحتمال عدم قدرة مزودي الخدمة الحاليين على مواصلة العمليات وتقديم الخدمات المطلوبة. ويجب أن تتضمن الخطة تحديد بدائل قابلة للاستمرار لاستئناف عملياتها في مجال تكنولوجيا المعلومات والاتصالات في أماكن أخرى.

الحوسبة السحابية (Cloud Computing) :

- الحوسبة السحابية هي نموذج خدمات ونقل معلومات لتمكين الوصول إلى الشبكة بحسب الطلب لمجموعة مُشتركة من موارد الحوسبة القابلة للتكوين (الخوادم والتخزين والخدمات). وقد لا يعرف مستخدمو مثل هذه الخدمات المواقع الدقيقة للخوادم والتطبيقات والبيانات داخل البنية الأساسية للحوسبة لمقدم الخدمة لاستضافة المعلومات وتخزينها ومعالجتها.
- عند القيام بالإجراءات لإرضاء المتطلبات لجميع ترتيبات عمليات الإسناد إلى مصادر خارجية (outsourcing) يجب أن تكون المؤسسة على دراية بالخصائص والمخاطر المميزة للحوسبة السحابية، ولا سيما في مجالات تكامل البيانات، والسيادة، والنزاهة، والاستئجارات المتعددة للمنصة، والاسترداد والسرية والامتثال التنظيمي، والتدقيق ونقل البيانات إلى الخارج.

- بما أن موردي خدمات الحوسبة السحابية قد يعتمدون الأساليب الممزوجة والإيجارات المتعددة من أجل معالجة بيانات الزبائن فيجب على المؤسسة الانتباه إلى قدرات مزودي الخدمة وتحديد بيانات الزبائن وأصول النظام بشكل واضح من أجل حمايتها.
- في حالة انتهاء العقد مع مزود الخدمة، سواء عند إنتهاء الصلاحية أم قبل المدة المحددة، يجب أن تمتلك المؤسسة السلطة التعاقدية والوسائل اللازمة لإزالة البيانات المخزنة على الفور في أنظمة مزود الخدمة والنسخ الاحتياطية.
- يجب على المؤسسة التحقق من قدرة مزود الخدمة على تعافي الأنظمة الخارجية وخدمات تقنية المعلومات، ضمن الهدف الزمني للتعافي المحدد قبل التعاقد مع مزود الخدمة.
- التأكد من توافر عناصر الأمان عند استخدام الحوسبة السحابية، وذلك من خلال:

(1) نظام إدارة هوية المستخدم.
(2) الحماية التامة للبيانات.
(3) خصوصية حفظ حقوق المستفيد.
(4) التزود بنظم أمن وحماية تمنع الاختراق.

تفادي سلبيات استخدام الحوسبة السحابية المحتملة:

(1) الاختراق غير المسموح به، وسرقة البيانات أو بيعها.
(2) انقطاع الخدمة بسبب انقطاع الإنترنت.
(3) تطبيقات دون المستوى المطلوب من الكفاية.

ثامناً: ضوابط حوكمة وإدارة المعلومات والتقنية ذات الصلة:

على المؤسسة القيام بتطوير دليل خاص لحوكمة وإدارة المعلومات والتقنية ذات الصلة، وقد يكون جزءا من دليل الحوكمة المؤسسية، بحيث يأخذ الدليل بالحسبان هذه الضوابط حدا أدنى، وبشكل ينسجم واحتياجاته وسياساته، وأن يتم اعتماد الدليل من المجلس، وتزويد المصرف المركزي به خلال مُدة أقصاها (6 أشهر) من تاريخ هذه الضوابط، وبحيث يعبر هذا الدليل عن نظرة المؤسسة الخاصة لحوكمة وإدارة المعلومات والتقنية ذات الصلة من حيث مفهومها وأهميتها ومبادئها الأساسية، وبشكل يراعي التشريعات وأفضل الممارسات الدولية بهذا الشأن، وعلى المؤسسة من خلال لجنة حوكمة تكنولوجيا المعلومات والاتصالات المنبثقة عن المجلس مراجعة هذا الدليل وتحديثه كلما اقتضت الحاجة.

المبادئ والسياسات وأطر العمل:

- على المجلس، أو من يُفَوّض من لجانه اعتماد منظومة المبادئ والسياسات وأطر العمل (Framework)اللازمة لتحقيق الإطار العام لإدارة موارد ومشاريع تقنية المعلومات والاتصالات وضبطها ومراقبتها، وبما يلبي متطلبات الأهداف وعمليات حوكمة تكنولوجيا المعلومات والاتصالات الواردة في المرفقين (2) و (3) على الترتيب.
- على المجلس، أو من يفوض من لجانه اعتماد المبادئ والسياسات وأطر العمل، وبصورة خاصة تلك المتعلقة بإدارة مخاطر تقنية المعلومات والاتصالات وإدارة أمن المعلومات وإدارة الموارد البشرية التي تلبي متطلبات عمليات حوكمة تكنولوجيا المعلومات والاتصالات الواردة في المرفق رقم (3)
- على المجلس، أو مَنْ يُقوّض من لجانه اعتماد منظومة السياسات اللازمة لإدارة موارد وعمليات حوكمة تكنولوجيا المعلومات والاتصالات الواردة في المرفق رقم (6)، وغد منظومة السياسات هذه حَدّاً أدنى، مع إمكانية الجمع والدمج لتلك السياسات بحسب ما تقتضيه طبيعة العمل على أن يتم تطوير سياسات أخرى ناظمة مواكبة لتطور أهداف المؤسسة وآليات العمل وعلى أن تحدد كل سياسة الجهة المالكة، ونطاق التطبيق، ودورية المراجعة والتحديث، وصلاحيات الاطلاع، والتوزيع، والأهداف والمسؤوليات وإجراءات العمل المتعلقة بها، والعقوبات في حال عدم الامتثال وآليات فحص الامتثال
- يراعي لدى إنشاء السياسات مساهمة جميع الشركاء الداخليين والخارجيين واعتماد أفضل الممارسات الدولية وتحديثاتها بوصفها مراجع لصياغة تلك السياسات مثل (COBIT, 31000 ISO/IEC 27001/2,ISO (ISO/IEC 9126, ISO/IEC 15504, ISO 22301, PCI DSS, ITIL,...etc

الهياكل التنظيمية:

- على المجلس إعتماد الهياكل التنظيمية (الهرمية واللجان) وبصورة خاصة تلك المتعلقة بإدارة موارد وعمليات ومشاريع تقنية المعلومات وإدارة امن المعلومات وإدارة الموارد البشرية التي تلبي متطلبات عمليات حوكمة تكنولوجيا المعلومات والاتصالات وتحقيق أهداف المؤسسة بكفاءة عالية وفعالية.
- يُراعى ضمان فصل المهام المتعارضة بطبيعتها ومتطلبات الحماية التنظيمية المتعلقة بالرقابة الثنائية حدا أدنى وكفاية وتحديث الوصف الوظيفي لدى اعتماد الهياكل التنظيمية للمؤسسة وتعديلها.

المعلومات والتقارير:

- على المجلس والإدارة التنفيذية العليا تطوير البنية التحتية ونظم المعلومات اللازمة لتوفير المعلومات والتقارير لمستخدميها بصفته مرتكزا لعمليات اتخاذ القرار في المؤسسة، وعليه يجب أن تتوافر متطلبات جودة المعلومات والمتمثلة بالمصداقية والنزاهة والتكامل والدقة والتوافرية (Integrity, Completeness, Accuracy and Validity) ومتطلبات السرية بحسب سياسة تصنيف البيانات والامتثال لتلك المعلومات والتقارير، فضلا عن المتطلبات الأخرى الواردة في المعيار (COBIT - Enabling Information) والمتمثلة بالموضوعية والمصداقية والسمعة والملاءمة والمبلغ المناسب والتمثيل المختصر، والتمثيل المتناسق، والتفسير، والفهم، وسهولة التلاعب والوصول المقيد (objectivity, believability, Reputation Relevancy Appropriate Amount, Concise Representation, Consistent Representation, Interpretability, understandability, Ease of manipulation, Restricted Access)
- على المجلس أو منْ يُقوّض من لجانه إعتماد منظومة المعلومات والتقارير الواردة في المرفق رقم (7)، وعد تلك المنظومة حدا أدنى مع مراعاة تحديد مالكين لتلك المعلومات والتقارير تحدد من خلالهم، وتفوض صلاحيات الاطلاع والاستخدام بحسب الحاجة للعمل والشركاء المعنيين على أن تتم مراجعتها وتطويرها بشكل مستمر لمواكبة تطوير أهداف وعمليات المؤسسة وبما يوافق أفضل الممارسات الدولية المقبولة بهذا الشأن.

الخدمات والبرامج والبنية التحتية لتكنولوجيا المعلومات والاتصالات:

- على المجلس أو من يفوض من لجانه والإدارة التنفيذية العليا اعتماد منظومة الخدمات والبرامج والبنية التحتية لتقنية المعلومات الواردة في المرفق رقم (8)، وعد تلك المنظومة هذا أدنى على أن يتم توفيرها وتطويرها بشكل مستمر لمواكبة تطور أهداف المؤسسة وعملياتها، وبما يوافق أفضل الممارسات الدولية المقبولة بهذا الشأن.
- على المجلس أو منْ يُفوّض من لجانه والإدارة التنفيذية العليا اعتماد منظومة الخدمات والبرامج والبنية التحتية لتقنية المعلومات والاتصالات الداعمة والمساعدة لتحقيق عمليات حوكمة تكنولوجيا المعلومات والاتصالات، ومن ثم اهداف المعلومات والتقنية المصاحبة لها، والأهداف المؤسسية.

المعارف والمهارات والخبرات:

- على المجلس أو من يفوض من لجانه اعتماد مصفوفة المؤهلات (HC Competences) وسياسات إدارة الموارد البشرية اللازمة لتحقيق متطلبات عمليات حوكمة تكنولوجيا المعلومات والاتصالات الواردة في المرفق رقم (3) ومتطلبات هذه الضوابط بشكل عام، وضمان وضع الشخص المناسب في المكان المناسب.
- على إدارة المؤسسة توظيف العنصر البشري المؤهل والمدرب من الاشخاص ذوي الخبرة في مجالات إدارة موارد تقنية المعلومات والاتصالات وإدارة المخاطر وإدارة أمن المعلومات وإدارة تدقيق تقنية المعلومات والاتصالات استناداً إلى معايير الخبرات الأكاديمية والفنية والمهنية من خلال تأشيرها من جهات ذات اختصاص على أن تتم إعادة تأهيل وتدريب الكوادر الموظفة حاليا لتلبية المتطلبات المذكورة خلال سنتين من تاريخ هذه الضوابط.
- على الإدارة التنفيذية في المؤسسة الاستمرار برفد موظفيها ببرامج التدريب والتعليم المستمر للحفاظ على مستوى من المعارف والمهارات يلبي ويحقق عمليات حوكمة تكنولوجيا المعلومات والاتصالات الواردة في المرفق رقم (3).
- على الإدارة التنفيذية في المؤسسة تضمين اليات التقييم السنوي للكوادر بمعايير قياس موضوعية تأخذ بالحسبان المساهمة من خلال المركز الوظيفي بتحقيق أهداف المؤسسة.

تاسعاً: إقتناء وتطوير نظم المعلومات والاتصالات:

- قد تفشل الكثير من الأنظمة بسبب ضعف في تصميم وتنفيذ النظام، فضلاً عن عدم كفاية الاختبارات؛ ولذلك يجب على المؤسسة تحديد أوجه القصور في النظام والعيوب في مراحل تصميم وتطوير واختبار النظام.
- ينبغي أن تنشئ المؤسسة لجنة توجيهية تتألف من أصحاب الشركات وفريق التطوير وغيرهم من المساهمين، من أجل توفير عمليات الإشراف ومراقبة تقدم المشروع، بما في ذلك الأهداف التي يجب تحقيقها في كل مرحلة من مراحل المشروع والأحداث المهمة التي سيتم الوصول إليها وفقا للجدول الزمني للمشروع وخطة تنفيذ المشروع (Project Plan)، وللمؤسسة تحديد الهيكلية الهرمية لتنفيذ كل مشروع.

إدارة التغييروتوثيق عملية التغيير:

- يجب أن تُنشئ المؤسسة عملية إدارة التغيير لضمان تقييم التغييرات في أنظمة الإنتاج والموافقة عليها وتنفيذها ومُراجعتها بطريقة خاضعة للرقابة.
- يجب تطبيق عملية إدارة التغيير على التغييرات المتعلقة بالنظام، ومكونات نظام الحماية، والإصلاحات الخاصة بالأجهزة، وتحديثات البرامج.
- قبل نشر التغييرات في بيئات الإنتاج يجب على المؤسسة إجراء تحليل للمخاطر والآثار لطلب التغيير فيما يتعلق بالبنية التحتية القائمة والشبكات ويجب على المؤسسة أيضا تحديد ما إذا كان التغيير الذي تم إدخاله سيؤدي إلى حدوث مشاكل أمنية أو مشاكل في توافق البرامج مع الأنظمة أو التطبيقات المتأثرة.
- يجب على المؤسسة اختبار التغيرات الوشيكة بشكل كاف وضمان قبوله من قبل المستخدمين قبل نقل النماذج التي تم تغييرها إلى نظام الإنتاج. ويجب أيضا تطوير وتوثيق خطط الاختبار المناسبة للتغيير الوشيك وأن تحصل المؤسسة على نتائج اختبار مع تسجيل دخول المستخدم قبل الترحيل.
- يجب أن تتم الموافقة على جميع التغييرات التي تطرأ على بيئات الإنتاج من قبل الموظفين المخولين للموافقة على طلبات التغيير.
- لتقليل المخاطر المرتبطة بالتغييرات، يجب عمل نسخ احتياطية من الأنظمة أو التطبيقات المتأثرة قبل التغيير ويجب أيضا وضع خطة التراجع للعودة إلى الإصدار السابق من النظام أو التطبيق في حالة مواجهة مشكلة أثناء النشر أو بعده، وأن تضع المؤسسة خيارات التعافي البديلة لمعالجة الحالات التي لا يسمح فيها التغيير للمؤسسة بالعودة إلى الحالة السابقة.
- سجلات التدقيق والحماية هي معلومات مفيدة لتسهيل عملية الإستجواب وكشف المشكلات. لذلك يجب على المؤسسة التأكد من تسهيل عملية الدخول لتسجيل النشاطات التي يتم تنفيذها أثناء عملية الترحيل.

مُتطلبات الحماية والإختبارات:

- يجب أن تُحَدِّد المؤسسة بوضوح مُتطلبات الحماية المُتعلقة في الوصول إلى النظام، والتوثيق، وترخيص المعاملات وسلامة البيانات وتسجيل نشاط النظام ومراجعة الحسابات وتتبع الأحداث الأمنية، ومعالجة الاستثناءات في المراحل المبكرة من تطوير النظام أو اقتنائه ويجب على المؤسسة أيضا إجراء فحص الامتثال لمعايير الحماية الخاصة بالمصارف ضد المتطلبات القانونية ذات الصلة.

- يجب وضع منهجية لاختبار النظام ويجب أن يغطي نطاق الاختبارات منطق الأعمال وضوابط الأمان وأداء النظام في ظل سيناريوهات الضغط المختلفة وظروف التعافي.
- يجب على المؤسسة التأكد من إجراء اختبار الانحدار الكامل قبل تصحيح أو تحسين النظام ويجب على المستخدمين الذين تتأثر أنظمتهم وأنشطتهم التشغيلية بتغييرات النظام مراجعة نتائج الاختبارات والموافقة عليها.
- يجب على المؤسسة إجراء اختبار القدرة على الاختراق قبل بدء تشغيل النظام الجديد لتوفير إمكانية الوصول إلى الإنترنت وواجهات الشبكة المفتوحة ويجب على المؤسسة أيضا إجراء فحص الضعف لمكونات الشبكة الخارجية والداخلية التي تدعم النظام الجديد.
- يجب أن تحتفظ المؤسسة ببيئات منطقية أو مادية منفصلة للوحدات والتكامل، فضلا عن النظام واختبار قبول المستخدم(UAT User Acceptance Testing) وأن تراقب عن كتب وصول المزودين والمطورين إلى بيئة اختبار قبول المستخدم ("UAT") .

مُراجعة رموز المصدر:

- هناك طرائق مختلفة لبرامج التشفير التي قد تخفي التهديدات الأمنية والثغرات سواء كانت متعمدة أم غير متعمدة عادة ما تكون اختبارات قبول النظام والمستخدم غير فعالة في اكتشاف الرموز الضارة، فايروسات، فإن اختبار الصندوق الأسود ليس أداة فعالة في تحديد أو كشف هذه التهديدات الأمنية ونقاط الضعف.
- مُراجعة رموز المصدر هي فحص منهجي لرمز المصدر للتطبيقات بهدف إيجاد عيوب ناجمة عن أخطاء في التشفير أو ممارسات ترميز ضعيفة أو هجمات خبيثة وهي مُصممة لتحديد مواطن الضعف وأوجه القصور الأمنية والأخطاء في تصميم النظام أو وظائفه المتعلقة بمجالات مثل هيكلية الرقابة والتحقق من صحة المدخلات ومعالجة الأخطاء وتحديث الملفات والتحقق من العوامل المتغيرة الوظيفية قبل تطبيق النظام.
- يجب أن تضمن المؤسسة وجود درجة عالية من تكامل النظام والبيانات للأنظمة كافة. ويجب أن تمارس المؤسسة الإجراءات لإرضاء المتطلبات للتأكد من أن تطبيقاتها لديها نظام رقابة مناسب، مع مراعاة نوع وتعقيد الخدمة التي تقدمها هذه التطبيقات.
- بناء على تحليل المخاطر في المؤسسة يجب أن يختبر النظام بشكل صارم وحدات تطبيق محددة إجراءات امنية مع مجموعة من مراجعة رموز المصدر واختبار الاستثناء ومراجعة الامتثال لتحديد

مُمارسات الترميز الخاطئة ونقاط ضعف الأنظمة التي قد تؤدي إلى حدوث مشاكل امنية والانتهاكات والحوادث.

تطوير المستخدم النهائي:

- هناك أدوات وبرامج تجارية شائعة تسمح للمستخدمين بتطوير تطبيقات بسيطة لأتمتة عملياتهم وإجراء تحليل البيانات وإصدار تقارير للمؤسسة والزبائن
- يجب على المؤسسة إجراء التقييم للتأكد من أهمية هذه التطبيقات للأعمال.
- ينبغي تنفيذ كثير من الإجراءات مثل حجم التعافي من الكوارث وصول المستخدم وضوابط حماية البيانات في الأقل من أجل تثبيت هذه التطبيقات
- تجب مراجعة واختبار رموز برامج تطوير المستخدم الأخير والبرامج النصية ووحدات الماكرو قبل استخدامها.لضمان سلامة التطبيقات وموثوقيتها.

عاشراً: إدارة مشاريع تكنولوجيا المعلومات والاتصالات:

- عند إعداد الإطار العام لإدارة المشروع، يجب على المؤسسة التأكد من أن المهام والعمليات الخاصة بتطوير أو الحصول على أنظمة جديدة تشمل تقييم وتصنيف مخاطر المشروع وعوامل النجاح الحاسمة لكل مرحلة من مراحل المشروع وتحديد المعالم الرئيسة للمشروع والنواتج، ويجب أيضاً أن تحدد المؤسسة بشكل واضح مهام ومسؤوليات الموظفين المشاركين في المشروع.
- يجب على المؤسسة توثيق الخطط بشكل واضح لجميع مشاريع تقنية المعلومات والاتصالات ويجب على المؤسسة أن تحدد بوضوح المخرجات التي يجب تحقيقها في كل مرحلة من مراحل المشروع، فضلا عن المعالم الأساسية التي يمكن الوصول إليها.
- يجب على المؤسسة التأكد من أن متطلبات المستخدم الوظيفية وحالات العمل وتحليل التكلفة مقابل المنفعة وتصميم الأنظمة والمواصفات الفنية وخطط الاختبار وتوقعات أداء الخدمة، يتم اعتمادها من قبل الإدارة المناسبة وإدارة تقنية المعلومات والاتصالات.
- يجب على المؤسسة أن تقوم بالإشراف الإداري على المشروع لضمان الوصول إلى الأهداف الأساسية وتحقيق النتائج في الوقت المناسب. ويجب أن تصعد المشكلات التي لا يمكن حلها على مستوى لجنة المشروع إلى الإدارة العليا للاهتمام والتدخل.

- يجب أن تكون هنالك بيئة تجريبية قبل تنفيذ المشروع في البيئة الفعلية لتجلب الأخطاء، وعدم التراجع والعودة إلى الإصدار السابق.

الحادي عشر: إدارة خدمات تكنولوجيا المعلومات والاتصالات:

يُعد الإطار لإدارة خدمة تكنولوجيا المعلومات والاتصالات ضرورياً لدعم أنظمة تقنية المعلومات والاتصالات وخدماتها وعملياتها وإدارة التغييرات والمشكلات، فضلاً عن الحفاظ على الإنتاج في بيئة تقنية المعلومات والاتصالات وينبغي أن يشتمل الإطار على هيكلية الإدارة والعمليات والإجراءات الخاصة بإدارة التغيير وإدارة إصدار البرامج وإدارة المشكلات والحوادث، فضلاً عن إدارة القدرات.

ترحيل البرامج:

- يتضمن ترحيل البرامج نقل الرموز والبرامج النصية من بينة البرمجة إلى بينات الاختبار والإنتاج. ويمكن أن تتسبب الرموز غير المصرح بها أو الضارة التي يتم حقنها أثناء عملية الترحيل في تعريض البيانات والأنظمة والعمليات للخطر في بيئة الإنتاج، لذا يجب القيام بالآتي:
- إنشاء بيئات منطقية أو مادية منفصلة لتطوير الأنظمة واختبارها وتنظيمها وإنتاجها.
- يجب إجراء تقييم للمخاطر وضمان تنفيذ ما يكفي من الرقابة الوقائية والعلاجية قبل توصيل البيئة غير الإنتاجية بالإنترنت
- يجب فرض مبدأ الفصل بين المهام بحيث لا يوجد فرد واحد لديه القدرة على تطوير وتجميع ونقل الرموز الموضوعة من بيئة إلى أخرى.
- بعد أن يتم تنفيذ التغيير بنجاح في بيئة الإنتاج، يجب أيضا أن يتم تكرار التغيير وترحيله إلى أنظمة التعافي من الكوارث أو تطبيقات العمليات التوافق.

إدارة الحوادث:

- يجب على المؤسسة إنشاء إطار لإدارة الحوادث بهدف استعادة خدمات تكنولوجيا المعلومات والاتصالات بشكل طبيعي باسرع ما يمكن بعد وقوع الحادث مع الحد الأدنى من التأثير في عمليات المؤسسة، ويجب أيضا تحديد مهام ومسؤوليات الموظفين المشاركين في عملية إدارة الحوادث التي تشمل تسجيل الحوادث وتحليلها ومُعالجتها ورصدها.

- تحصل الحوادث في تقنية المعلومات عندما يكون هناك خلل غير متوقع في موعد التسليم القياسي لخدمات نقدية المعلومات والاتصالات، ويجب على المؤسسة إدارة مثل هذه الحوادث بشكل مناسب لتفادي أية حالات سوء معالجة تؤدي إلى تعطيل طويل الأمد لخدمات تقنية المعلومات أو مزيد من التفاقم
- من المهم أن تتلاءم معالجة الحوادث بحسب مستوى الخطورة المناسب بوصفه جزءاً من تحليل الحوادث، ويجوز للمؤسسة أيضاً إنتداب وظيفة لتحديد وتعيين مستوى خطورة الحوادث إلى وظيفة مكتب المساعدة الفني الرئيس. ويجب على المؤسسة تدريب موظفي مكتب المساعدة على تمييز الحوادث ذات مستوى الخطورة المرتفع فضلا عن ذالك. يجب تحديد وتوثيق المعايير المستخدمة لتقديم مستويات خطورة الحوادث.
- يجب على المؤسسة وضع إجراءات التصعيد والقرار المقابلة إذ يتناسب الإطار الزمني للقرار مع مستوى خطورة الحادث ويجب اختبار خطة التصعيد والاستجابة المحددة مسبقا للحوادث الأمنية على أساس منتظم.
- يجب تشكيل فريق استجابة طوارئ الحواسيب يضم موظفين داخل المؤسسة مع المهارات الفنية والتشغيلية اللازمة للتعامل الحوادث الكبرى.
- في بعض الحالات قد تتطور الحوادث الأساسية بشكل سلبي في المواقف الحرجة، ويجب إبقاء الإدارة العليا على علم تام بتطور هذه الحوادث بحيث يمكن اتخاذ قرار تفعيل خطة التعافى من الكوارث في الوقت المناسب، ويجب أن تقوم المؤسسات المصرفية بإبلاغ المصرف المركزي باسرع وقت ممكن في حالة فشل النظام في استعادة القدرة على العمل بعد الكوارث وأن يتم إنشاء إجراءات لإبلاغ مصرف ليبيا المركزي عن هذه الحوادث.
- قدرة المؤسسة على الحفاظ على ثقة الزبائن خلال الأزمات أو حالات الطوارئ لها أهمية كبيرة فيما يخص سمعة المؤسسة وسلامتها. ويجب أن تضمن المؤسسات إجراءات الاستجابة للحوادث وخطة عمل محددة مسبقة لمعالجة قضايا العلاقات العامة.
- يجب على المؤسسة إبقاء الزبائن على علم بأية حوادث مهمة قد تحصل. ويجب تقييم فعالية طرائق الاتصال، بما في ذلك إعلام الجمهور عند الضرورة.
- وبما أن الحوادث قد تنبع من كثير من العوامل، فيجب إجراء تحليل جذري للأسباب والأحداث الهامة التي تؤدي إلى تعطيل شديد للخدمات واتخاذ إجراءات علاجية لمنع تكرار حوادث مماثلة

- يجب على المؤسسة أن تضمن تقرير الحوادث الخاص بها، فضلاً عن ملخص تنفيذي للحدث، وتحليلاً للأسباب الجذرية وتأثيرات الحوادث، فضلاً عن التدابير المتخذة لمعالجة الأسباب الجذرية للحدث الذي يجب أن يغطي ما يلي:

أ- تحليل السبب الجذري:

- متى حدث ذلك؟
- أين حدث؟
- لماذا وكيف وقع الحادث؟
- كم مرة وقعت حادثة مُماثلة خلال السنوات الثلاث الماضية ؟
- ما هى الدروس المُستفادة من هذا الحادث؟

ب- تحليل التأثيرات:

- مدى تأثير الحادث ومدته ونطاقه بما في ذلك المعلومات المتعلقة بالنظم والموارد والزبائن المتأثرين حجم الحادث بما في ذلك الإيرادات والخسائر والتكاليف والاستثمارات وعدد الزبائن المتأثرين والآثار المترتبة على السمعة والثقة.
- خرق الشروط والإجراءات التنظيمية نتيجة للحادث.

ج - التدابير التصحيحية والوقائية:

- يجب إتخاذ إجراء تصحيحي فوري لمعالجة عواقب الحوادث.
- ينبغي إعطاء الأولوية لمعالجة اهتمامات الزبائن أو تعويضهم
- وضع لمعالجة الأسباب الجذرية للحادث.
- وضع لمنع وقوع حوادث مماثلة أو ذات صلة.
- يجب على المؤسسة معالجة جميع الحوادث بشكل كاف ضمن الإطار الزمني للحلول المتماثلة ومُراقبة جميع الحوادث لحلها.

إدارة المشكلة:

- في حين أن الهدف من إدارة الحوادث هو إستعادة خدمة تكنولوجيا المعلومات والاتصالات في أقرب وقت مُمكن، فإن الهدف من إدارة المشاكل هو تحديد السبب الجذري للمشكلة والقضاء عليه لمنع حدوث مثل هذه المشاكل المتكررة.

- يجب أن تحدد المؤسسة المهام والمسؤوليات بشكل واضح للموظفين المشاركين في عملية إدارة المشكلات وتحديد وتصنيف وإعطاء الأولويات ومعالجة جميع المشاكل في الوقت المناسب.
- يجب أن تحدد المؤسسة بشكل واضح معايير تصنيف المشاكل بحسب مستوى الخطورة، لتسهيل عملية التصنيف من أجل الرقابة على المشكلات وتخفيفها بفاعلية، ويجب على المؤسسة تحديد الهدف من وقت القرار المستهدف، فضلا عن عمليات التصعيد المناسبة لكل مستويات الخطورة
- ينبغي إجراء تحليل الاتجاهات للحوادث السابقة لتسهيل تحديد المشاكل المماثلة والوقاية منها.

إدارة القدرات:

- لضمان قدرة أنظمة تقنية المعلومات والاتصالات والبنية التحتية الخاصة بها على دعم وظائف العمل، ينبغي للمؤسسة مراقبة ومراجعة مؤشرات مثل الأداء والقدرة والاستغلال الكامل للموارد.
- يجب أن تُنشئ المؤسسة عمليات مُراقبة وإحتساب النسب والحد الأدنى والأعلى لتوفير الوقت الكافي للمؤسسة من أجل عمليات التخطيط وتحديد الموارد الإضافية لتلبية المتطلبات التشغيلية والتجارية بفعالية.

الثاني عشر: موثوقية الأنظمة وتو افرها وإسترجاعها:

- تُعد الموثوقية والتوافرية والاسترجاع الخاصة بأنظمة تقنية المعلومات والاتصالات والشبكات والبنى التحتية حاسمة في الحفاظ على الثقة والائتمان في القدرات التشغيلية والوظيفية للمؤسسة عندما تفشل الأنظمة الحماسة، عادة ما يكون الأثر في عمليات المؤسسة أو الموظفين شديدًا وواسع الانتشار، وقد تتعرض المؤسسة لعواقب وخيمة على سمعتها جراء ذلك.
- يجب على المؤسسة تحديد أولويات الاسترداد واستئناف الأعمال واختبار وممارسة إجراءات الطوارئ حتى يتم تقليل المشكلات الناشئة عن الحوادث الخطيرة.

تو افرية النظام:

- وتتمثل العوامل الرئيسية المُرتبطة بالحفاظ على توافر النظام بشكل مرتفع في القدرات الكافية والأداء ذي مُصداقية ووقت الاستجابة السريع وقابلية التوسع والقدرة على التعافي السريع.

- يجوز للمؤسسة توظيف عدد من مكونات الأنظمة والشبكات المعقدة المترابطة لمعالجة تقنية المعلومات والاتصالات الخاصة بها، ويجب على المؤسسة تطوير عمليات رقابة زيادة عن حدها لتقليل الأخطاء الفردية التي يمكن أن تتسبب في سقوط الشبكة بالكامل، وأن تحتفظ المؤسسة بمكونات الأجهزة والبرمجيات والشبكات الاحتياطية الضرورية من أجل التعافي السريع.
- يجب على المؤسسة تحقيق مستوى عال من التوافرية للأنظمة الحسّاسة.

خطة التعافي من الكوارث:

- عند صياغة خُطة التعافي السريع وبنائها، يجب أن تقوم المؤسسة بتحليل للسيناريوهات ومُعالجة مُختلف أنواع سيناريوهات الطوارئ الأخرى، وأن تنظر المؤسسة في سيناريوهات مثل حالات انقطاع الخدمة عن النظام الرئيس التي قد تنتج عن أخطاء في النظام، أو خلل في الأجهزة، أو أخطاء تشغيلية أو حوادث أمنية.
- يجب أن تقوم المؤسسة بتقييم خطة التعافي وإجراءات الاستجابة للحوادث مرة كل سنة في الأقل، وتحديثها عندما تحدث تغييرات في العمليات والأنظمة وشبكات الأعمال.
- ينبغي على المؤسسة تنفيذ عمليات النسخ الاحتياطي والقدرة على التعافي السريع على مستوى النظام الفردي أو على مستوى المجموعات ويجب الأخذ بالحسبان الترابط بين الأنظمة الحسّاسة في رسم خطة التعافي وإجراء اختبارات الطوارئ.
- يجب على المؤسسة تحديد أولويات تعافي النظام، واستئناف الأعمال، ووضع أهداف استرداد محددة، بما في ذلك موضوعية نقطة التعافي (RTO) لأنظمة تقنية المعلومات والاتصالات وتطبيقاتها نقطة التعافي المستهدفة (RTO) هي المدة الزمنية من نقطة الانقطاع والتي يجب استعادة النظام خلالها تشير نقطة التعافي المستهدفة (RPO) إلى مقدار مقبول من البيانات المفقودة لنظام تقنية المعلومات والاتصالات في حالة حدوث كارثة.
- يجب على المؤسسة إجراء عمليات التعافي في موقع منفصل جغرافيا عن الموقع الأساس حتى يتمكن من استعادة الأنظمة الحساسة واستئناف العمليات التجارية في حالة حدوث عطل في الموقع الأساس
- يجب على المؤسسة التأكد من تركيز عمليات الشبكة العابرة للحدود مع استراتيجيات أخرى مثل مشاركة مزودي خدمة الشبكة المختلفة ومسارات الشبكة البديلة التي يتم تأسيسها.

إختبارات التعافي من الكوارث:

- أثناء انقطاع الخدمة عن النظام، يجب على المؤسسة الامتناع عن اعتماد تدابير التعافي غير المجدية وغير المجربة على إجراءات التعافي المحددة مسبقا، والتي تم التدرب عليها والموافقة عليها من قبل الإدارة وتنطوي تدابير التعافي المخصصة على مخاطر تشغيلية عالية إذ لم يتم التحقق من فعاليتها من خلال الاختبارات الصارمة والتحقق من صحتها.
- يجب على المؤسسة الاختبار والتحقق في الأقل سنويا من فعالية متطلبات التعافي وقدرة الموظفين على تنفيذ إجراءات الطوارئ والتعافي الضرورية.
- يجب تغطية سيناريوهات مختلفة، بما في ذلك إيقاف التشغيل الكلي أو تعطل الموقع الرئيس، فضلا عن فشل مكونات النظام الفردي أو على مستوى المجموعات في اختبارات التعافي بعد الكوارث.
- يجب على المؤسسة إختبار عمليات التعافي من خلال اعتماد الأنظمة المختلفة. وينبغي إجراء إختبار التعافي الثنائي أو المتعدد الأطراف إذ ترتبط الشبكات والأنظمة بمقدمي خدمات ومزودين محددين.
- يجب على المؤسسة إشراك مستخدمي الأعمال في تصميم وتنفيذ حالات اختبار شاملة للتحقق من أن الأنظمة المتعافية تعمل بشكل صحيح، وإشراكهم في اختبارات التعافي بعد الكوارث التي يجريها مقدمو الخدمة، بما في ذلك تلك الأنظمة الموجودة في الخارج.

إدارة النسخ الاحتياطية للبيانات:

- يجب على المؤسسة تطوير استراتيجية النسخ الاحتياطي للبيانات لتخزين المعلومات المهمة من خلال تطبيق أساليب. تخزين بيانات محددة، مثل أنظمة التخزين المتصلة المُباشرة (DAS)، أو أنظمة التخزين المتصلة بالشبكة (NAS) أو أنظمة التخزين المحلية الفرعية المتصلة بخوادم الإنتاج (SAN).
- يجب على المؤسسة إجراء إختبارات دورية وإختبارات التحقق من استرداد النسخ الاحتياطية وتقييم ما إذا كانت وسائط النسخ الاحتياطي كافية وفعالة بما فيه الكفاية لدعم عمليات التعافي في المؤسسة.
- يجب على المؤسسة تشفير الأشرطة والأقراص الخاصة بالنسخ الاحتياطية، بما في ذلك وحدات الخزن المُتنقلة USB، التي تحتوي على معلومات حساسة وسرية قبل نقلها خارج الموقع للتخزين.

الثالث عشر: إدارة أمن البنية التحتية التشغيلية:

- إن نظام تقنية المعلومات عرضة لأشكال مُختلفة من الهجمات الإلكترونية، وتزايد وتكرار الهجمات الخبيثة؛ لذا من الضروري أن تقوم المؤسسات المصرفية بتنفيذ حلول أمنية في البيانات والتطبيقات وقواعد البيانات وانظمة التشغيل وطبقات الشبكة لمعالجة هذه التهديدات و احتواؤها بشكل ملائم.
- ويجب تنفيذ التدابير المناسبة لحماية المعلومات الحساسة والسرية مثل بيانات العميل الشخصية والحسابات والمعاملات التي يتم تخزينها ومعالجتها في الأنظمة، ويجب أيضا أن تتم عملية التصديق على الزبائن بشكل صحيح قبل الوصول إلى المعاملات من خلال الإنترنت والمعلومات شخصية ومعلومات الحسابات الحساسة ويجب تأمين معلومات الزبائن الحساسة بما في ذلك بيانات اعتماد تسجيل الدخول، وكلمات المرور، وأرقام التعريف الشخصية (PINS)، ضد عمليات الاستغلال مثل: إحتيال البطاقات الائتمانية، واستنساخ البطاقات والقرصنة، والتَصَيُّد والبرامج الضارة.

منع فقدان البيانات:

- من المُحتمل أن يكون التخريب الداخلي أو التَجَسُّس السري أو الهجمات العنيفة التي يقوم بها الموظفون والمتعاقدون والمزودون الموثوق بهم من بين أخطر المخاطر التي يمكن أن تواجهها المؤسسات المصرفية في بيئة تقنية معلومات ديناميكية ومُعقدة بشكل متزايد يتميز الموظفون الحاليون والسابقون والمتعاقدون والمزوّدون وأولئك الذين لديهم معرفة بالأعمال الداخلية لأنظمة المؤسسة، والعمليات والرقابة الداخلية على المهاجمين الخارجيين ولا يُعرض الهجوم الناجح ثقة الزبائن في أنظمة وعمليات الرقابة الداخلية للمؤسسة فحسب، بل يتسبب أيضا في خسارة مالية حقيقية عندما يتم الكشف عن الأسرار التجارية والمعلومات الخاصة بالمؤسسة يجب أن تحدد المؤسسة البيانات المهمة وأن تعتمد تدابير مناسبة لاكتشاف ومنع الوصول غير المخول أو النسخ، أو نقل المعلومات السرية.
- يجب على المؤسسة تطوير استراتيجية شاملة لمنع فقدان البيانات لحماية المعلومات الحساسة والسرية، مع مراعاة النقاط الآتية:

1. البيانات عند نقطة النهاية: البيانات الموجودة في أجهزة الكمبيوتر المحمولة وأجهزة الكمبيوتر الشخصية وأجهزة التخزين المحمولة والأجهزة المحمولة.

2. البيانات فيد الحركة: البيانات التي تمر عبر الشبكة أو يتم نقلها بين المواقع.
3. البيانات الأخرى: البيانات في الحواسيب المخزنة التي تشمل الملفات المخزنة على الخوادم وقواعد البيانات ووسائل الإعلام الاحتياطية ومنصات التخزين.

- لتحقيق أمن البيانات في نقط النهاية، ينبغي للمؤسسة تنفيذ التدابير المُناسبة لمُعالجة مخاطر سرقة البيانات وفقدان البيانات وتسربها من أجهزة نقطة النهاية ومواقع خدمة الزبائن ومراكز الاتصال وحماية المعلومات السرية المخزنة في جميع أنواع أجهزة نقط النهاية مع التشفير المتين.
- يجب الا تستخدم المؤسسة خدمات الإنترنت غير الأمنة مثل مواقع التواصل الاجتماعي ومواقع تخزين عبر الإنترنت ورسائل البريد الإلكتروني للتواصل وتخزين المعلومات السرية وتنفيذ التدابير التي من شأنها منع استخدام هذه الخدمات داخل المؤسسة وكشفها.
- من أجل تبادل المعلومات السرية بين المؤسسة وأطرافها الخارجية، يجب على المؤسسة الحرص على الحفاظ على سرية جميع المعلومات الحماسة ، واتخاذ التدابير المناسبة في جميع الأوقات بما في ذلك إرسال المعلومات من خلال القنوات المشفرة (على سبيل المثال عبر بروتوكول البريد المشفر) أو تشفير البريد الإلكتروني والمحتويات باستخدام التشفير المتين بحسب قوة المفتاح الكافية وإرسال مفتاح التشفير عبر قناة إرسال منفصلة إلى المتسلمين المستهدفين. بدلاً من ذلك قد تختار المؤسسة وسائل أمنة أخرى لتبادل المعلومات السرية مع المستلمين المستهدفين.
- يجب تشفير وحماية المعلومات السرية المخزنة على أنظمة التقنية والخوادم وقواعد البيانات من خلال ضوابط قوية للوصول، مع الأخذ بالحسبان مبدا "الأقل امتيازا".
- يجب على المؤسسة تقييم الطرائق المختلفة التي يمكن من خلالها إزالة البيانات بأمان من وسائط التخزين وتنفيذ التدابير لمنع فقدان المعلومات السرية ويجب على المؤسسة أن تأخذ بالحسبان المتطلبات الأمنية للبيانات الموجودة في وسائل الإعلام.

إدارة تحديث تكنولوجيا المعلومات والاتصالات:

- لتسهيل تتبع موارد تكنولوجيا المعلومات والاتصالات، يجب على المؤسسة الاحتفاظ بقائمة محدثة من مكونات البرامج والأجهزة المستخدمة في بيئات الإنتاج والتعافي من الكوارث، والتي تشمل جميع الضمانات المرتبطة بها وعقود الدعم الأخرى ذات الصلة بمكونات البرامج والأجهزة.
- يجب على المؤسسة إدارة نظم تقنية المعلومات والاتصالات وبرامجها بشكل فعال، بحيث يتم استبدال الأنظمة القديمة وغير المدعومة التي تزيد احتمالية تعرضها للمخاطر الأمنية في الوقت

المناسب ويجب على المؤسسة أيضا أن تولي تاريخ انتهاء دعم المنتج (EOS) عناية فائقة، إذ أنَّ من الشائع أن يتوقف المزودون عن تقديم التصحيحات بما في ذلك تلك المتعلقة بمواطن الثغرات التي يتم اكتشافها بعد تاريخ انتهاء دعم المنتج (EOS).

- يجب على المؤسسة وضع خطة تحديث للتقنية لضمان استبدال الأنظمة والبرامج في الوقت المناسب وإجراء تقييم للمخاطر للنظم التي تقترب من تواريخ انتهاء دعم المُنتج (EOS) لتقييم مخاطر إستمرارية الاستخدام وإنشاء ضوابط فعالة للتخفيف من المخاطر عند الضرورة.

إدارة تكوين الحماية والشبكات:

- يجب على المؤسسة تكوين أنظمة تقنية المعلومات والاتصالات والأجهزة مع إعدادات الأمان التي توافق مستوى الحماية المتوقع ووضع معايير أساسية لتسهيل التناسق في التطبيقات الثابت لتكوينات الأمان على أنظمة التشغيل وقواعد البيانات وأجهزة الشبكة والأجهزة المحمولة للمؤسسات في بيئة تقنية المعلومات والاتصالات.
- ينبغي أن تجري المؤسسة فحوصات منتظمة للتأكد من أن المعايير الأساسية تطبق بشكل موحد، ويتم الكشف حالات عدم الامتثال ورفعها للتحقيق إن تكرار مراجعات التقوية يتناسب ومستوى مخاطر الأنظمة.
- يجب على المؤسسة تثبيت برامج مكافحة الفيروسات على الخوادم إن أمكن ومحطات العمل وتحديث ملفات برامج مكافحة الفيروسات بشكل منتظم وإنشاء جداول الفحص التلقائي للفيروسات على الخوادم ومحطات العمل بشكل منتظم
- ينبغي أن تقوم المؤسسة بتثبيت أجهزة حماية الشبكات مثل الجدران النارية، التي من المفضل أن تكون مزدوجة ومن مجهزين مختلفين كي تزيد من صعوبة الاختراق بدرجة أكبر، وكذلك أنظمة كشف التسلل ومنعه في المراحل الحاسمة من البنية التحتية لتقنية المعلومات والاتصالات لحماية محيط الشبكة. يجب على المؤسسة نشر الجدران النارية أو إجراءات أخرى مماثلة داخل الشبكات الداخلية لتقليل تأثيرات الأمنية الناشئة من أنظمة خارجية، وكذلك من الشبكة الداخلية الموثوقة يجب على المؤسسة أن تقوم على بمراجعة القواعد الخاصة بأجهزة حماية الشبكات أساس منتظم لتحديد ما إذا كانت هذه القواعد مناسبة وملائمة.
- عندما تختار المؤسسة نشر شبكات المناطق المحلية اللاسلكية (WLAN) داخل المؤسسة فإن عليها أن تكون على دراية بالمخاطر المرتبطة بهذه البيئة ويجب تنفيذ جملة من الإجراءات الوقائية من الاختراق مثل بروتوكولات الاتصال الأمنة بين نقط الوصول والزبائن المتصلين لاسلكيا، لتأمين

الشبكة من الوصول غير المصرح به، وعليها أن تنشأ شبكات محلية منفصلة لأقسام المؤسسة من جانب وتلك التي يتمكن زبائن المؤسسة والأشخاص الخارجيين من الوصول إليها من جانب آخر.

تقييم الضعف وإختبارات الاختراق:

- تقييم الضعف (VA) هو عملية تحديد وتقييم واكتشاف نقط الضعف في النظام والقيام بالاختبارات بانتظام للكشف عن الثغرات الأمنية في بيئة تقنية المعلومات والاتصالات
- يجب على المؤسسة نشر مجموعة من الأدوات الآلية والتقنيات البدوية لأداء عمليات تقييم الضعف (VA) بشكل شامل فيما يخص الويب المعتمد على أنظمة الواجهة الخارجية يجب أن يشمل نطاق تقييم الضعف (VA) الثغرات المشتركة للويب مثل حقن النصوص عبر المواقع (SQL)
- يجب أن تقوم المؤسسة بعمليات لمعالجة المشكلات التي تم تحديدها في تقييم الضعف (VA)، ويجري التحقق من الصحة بعد ذلك للتحقيق على أن الفجوات تتم معالجتها بالكامل.
- يجب على المؤسسة إجراء إختبارات الاختراق من أجل إجراء تقييم متعمق لوضع الأمن في النظام من خلال محاكاة الهجمات الفعلية على النظام، وإجراء اختبارات الاختراق على الأنظمة المتصلة بالإنترنت في الأقل بشكل سنوي.

إدارة التصحيح:

- يجب أن تقوم المؤسسة بإجراءات إدارة التصحيح بما في ذلك تحديد وتصنيف وترتيب أولويات التصحيح لتنفيذ تصحيحات الحماية في الوقت المناسب، يجب على المؤسسة تحديد الإطار الزمني للتنفيذ لكل فئة من إجراءات التصحيح.
- من أجل تطبيق التصحيح، إذا لم يتم تنفيذها بشكل مناسب يمكن أن يؤثر ذلك على الأنظمة الفرعية الأخرى ويجب على المؤسسة أيضا إجراء اختبار صارم لعمليات التصحيح قبل النشر في بيئة الإنتاج.

المُر اقبة الأمنية:

- المراقبة الأمنية هي وظيفة مُهمة في بيئة تقنية المعلومات والاتصالات للكشف عن الهجمات الضارة على أنظمة تقنية المعلومات والاتصالات، ولتسهيل الكشف الفوري عن النشاطات غير المصرح بها

أو الخبيثة من قبل الأطراف الداخلية والخارجية، يجب إنشاء أنظمة وعمليات مراقبة أمنية مناسبة.

- يجب على المؤسسة تنفيذ إجراءات المراقبة والإشراف على الشبكات باستخدام أجهزة أمن الشبكات، مثل أنظمة كشف ومنع التسلل لحماية المؤسسة من هجمات تسلسل الشبكة وكذلك استخدام الإنذارات عند حدوث أي تدخل.
- يجب على المؤسسة استخدام أدوات مراقبة تمكن من اكتشاف التغييرات في موارد التقنية الأساسية مثل قواعد البيانات أو ملفات النظام أو البيانات، لتسهيل التعرف على التغييرات غير المصرح بها.
- يجب على المؤسسة إجراء عمليات مراقبة للوقت الحقيقي للأحداث الأمنية للأنظمة والتطبيقات الحيوية، لتسهيل الكشف الفوري عن النشاطات الضارة على هذه الأنظمة والتطبيقات.
- يجب على المؤسسة مراجعة سجلات الحماية للأنظمة والتطبيقات وأجهزة الشبكة بشكل منتظم من أجل الحالات الشاذة.
- يجب على المؤسسة حماية سجلات النظام والاحتفاظ بها بشكل ملائم لتسهيل عمليات التحقيق في المستقبل. وعند تحديد مدة الاحتفاظ السجلات، يجب أن تأخذ المؤسسة بالحسبان المتطلبات القانونية للاحتفاظ بالوثائق وحمايتها.

الرابع عشر: حماية مراكز البيانات والرقابة عليها:

- نظراً إلى أن الأنظمة والبيانات حسّاسة ومُرَكَّزة ومحفوظة في مراكز البيانات فمن المهم أن تكون مراكز البيانات مرئة ومحمية ماديا من التهديدات الداخلية والخارجية.

تقييم مخاطر التهديد والحساسية:

- إن الغرض من تقييم مخاطر التهديد والضعف ("TVRA") هو تحديد التهديدات الأمنية ونقط الضعف التشغيلية في مراكز البيانات وذلك لتحديد مستوى ونوع الحماية التي ينبغي وضعها للحماية من هذا المخاطر.
- يختلف تقييم مخاطر التهديد والضعف المتعلقة بمراكز البيانات بناءً على عدد من العوامل مثل أهمية مراكز البيانات والموقع الجغرافي والاستئجارات المتعددة ونوع المستاجر بن الذين يشغلون مراكز البيانات وتأثير الكوارث الطبيعية والسياسات الاقتصادية والاجتماعية وأثر الكوارث

الطبيعية والمناخ السياسي والاقتصادي للبلد الذي يقيم فيه، وأن ترتكز المؤسسة على تقييم مخاطر التهديد والضعف (TVRA) الخاص بها على مختلف السيناريوهات المحتملة للتهديدات التي تشمل السرقة والانفجارات والحرق المتعمد والدخول غير المصرح به، والهجمات الخارجية والتخريب من الداخل.

- يجب على المؤسسة أن تضمن في نطاق تقييم مخاطر التهديد والضعف (TVRA) مراجعة محيط مراكز البيانات والبيئة المحيطة، فضلا عن المبنى ومرافق مراكز البيانات ومراجعة الإجراءات الأمنية اليومية، والنظم الميكانيكية والهندسية الحساسة والبناء والعناصر الهيكلية وكذلك ضوابط الوصول المادية والتشغيلية والمنطقية.
- عند اختيار مزودي مراكز البيانات يجب على المؤسسة الحصول على تقرير تقييم مخاطر التهديد والضعف ("TVRA") وتقييمه على مرافق مركز البيانات يجب أن تتحقق المؤسسة من أن تقارير تقييم مخاطر التهديد والضعف ("TVRA") محدثة، وأن مزؤدي مراكز البيانات ملتزمون بمعالجة جميع نقط الضعف المادية المحددة.

فيما يخص المؤسسة التي يختار بناء وتطوير مراكز البيانات الخاصة بها، يجب إجراء تقييم للتهديدات ونقط الضعف في مرحلة دراسة الجدوى.

الحماية المادية:

- يجب على المؤسسة تقييد الوصول إلى مراكز البيانات للموظفين المخولين فقط وأن يتم منح الوصول إلى مراكز البيانات بناءً على الحاجة إليها، ويجب أيضاً إلغاء وصول الموظفين إلى مراكز البيانات فوراً إذا لم تُعد هناك حاجة إليهم.
- فيما يخص الموظفين غير المرتبطين بمراكز البيانات مثل المزودين ومسؤولي النظام والمهندسين الذين قد يحتاجون إلى وصول مؤقت إلى مراكز البيانات للقيام بأعمال صيانة وإصلاح يجب على المؤسسة ضمان وجود إشعار وموافقة مناسبة لهؤلاء الموظفين من أجل هذه الزيارات والتأكد من أن الزوار يرافقون في جميع الأوقات من قبل موظف معتمد من مراكز البيانات.
- يجب ضمان أن المحيط الخارجي لمراكز البيانات والمباني وغرفة المعدات تم تأمينها ومراقبتها ماديا ويجب استخدام نظم رقابة مادية وبشرية وإجراءات مثل استخدام حراس الأمن وأنظمة الوصول إلى البطاقات والحواجز عند الحاجة. يجب نشر أنظمة الحماية وأدوات المراقبة عند الحاجة لمراقبة وتسجيل النشاطات التي تجري داخل مراكز البيانات. وأن تضع تدابير أمنية لمنع الوصول غير المصرح به إلى الأنظمة ورفوف المعدات والأشرطة.

مُرونة مركز البيانات:

- لتحقيق مرونة في مراكز البيانات يجب عدم التغاضي عن بعض الأخطاء في مجالات محددة مثل الطاقة الكهربائية وتكييف الهواء وأدوات إخماد الحريق وإتصالات البيانات.
- يجب على المؤسسة فرض الرقابة على البيئة بشكل منتظم وصارم داخل مراكز البيانات تعد مراقبة الظروف البيئية مثل درجة الحرارة والرطوبة داخل مراكز البيانات أمرًا بالغ الأهمية لضمان وقت التشغيل وموثوقية النظام وتصعيد أي خلل يتم اكتشافه إلى الإدارة وحل المشكلة في الوقت المُناسب.
- يجب تنفيذ أنظمة الحماية والإخماد الآلي للحرائق في مراكز البيانات للسيطرة على الحرائق كاملة في حالة نشوبها ويجب أيضا تثبيت كاشفات الدخان وأدوات إخماد الحريق المحمولة في مراكز البيانات
- للتأكد من وجود طاقة احتياطية كافية، يجب تثبيت مصادر طاقة احتياطية تحتوي على مصادر طاقة غير منقطعة وانظمة البطاريات ومولدات الديزل.
- اعتماد المعايير والمواصفات القياسية العالمية لمراكز البيانات (DATA CENTER) الواردة في المرفق رقم (8).

الخامس عشر: الرقابة على الوصول للموارد:

هُناك ثلاثة من أهم مبادئ الحماية للأنظمة الداخلية وهي:

- مبدأ عدم العمل المنفرد - بعض وظائف الأنظمة وإجراءاتها ذات طبيعة حماسة وحرجة بحيث يجب على المؤسسات المصرفية التأكد من تنفيذها من قبل أكثر من شخص واحد في الوقت نفسه، أو تنفيذها من قبل شخص واحد وفحصها من قبل شخص آخر. وقد تتضمن هذه الوظائف تهيئة الأنظمة الحساسة وتكوينها، وإنشاء مفاتيح التشفير واستخدام الحسابات الإدارية.
- مبدأ الفصل بين المهام - يُعد الفصل بين المهام عنصرا أساسيا في الرقابة الداخلية. يجب أن تضمن المؤسسة أن المسؤوليات والواجبات الخاصة بأنظمة التشغيل وتصميم وتطوير الأنظمة وبرامج صيانة للتطبيقات وإدارة الرقابة على الوصول للموارد وأمن البيانات وأمناء وملفات النسخ الاحتياطية يتم فصلها وتنفيذها من قبل مجموعات مختلفة من الموظفين واله يجب أن يتم تنظيم تناوب الوظائف وعمليات التدريب لوظائف الإدارة الأمنية ويجب على المؤسسة تصميم عمليات

المعاملات بحيث لا يجوز لأي شخص أن يقوم بالمعاملات ويوافق عليها وينفذها ويدخلها إلى النظام لغرض استمرار الاحتيال أو بطريقة تخفي تفاصيل العملية.

- مبدأ الرقابة على الوصول للموارد يجب على المؤسسة فقط منح الوصول والامتيازات للنظام على أساس المسؤولية الوظيفية وضرورة الالتزام بالواجبات ويجب أن تتحقق المؤسسة من أنه لا يجوز لأي شخص بحكم منصبه.

ان يكون له أي حق في الوصول إلى البيانات السرية والتطبيقات وموارد النظام والمرافق وأن تسمح فقط للموظفين المُخَوَّلين للوصول إلى المعلومات السرية واستخدام موارد النظام فقط لأغراض مشروعة.

إدارة وصول المُستخدمين:

- يجب على المؤسسة منح الوصول إلى الأنظمة والشبكات فقط على أساس الحاجة إلى الاستخدام وخلال المدة التي يكون فيها الوصول مطلوبا والتأكد من إعطاء أصحاب الموارد الإذن والموافقة على جميع طلبات الوصول إلى الموارد.
- إن المزودين ومقدمي الخدمات الذين يمتلكون صلاحيات التخويل بالوصول إلى أنظمة المؤسسة الحساسة وموارد الحواسيب الأخرى، يشكلون مخاطر مماثلة مثل المخاطر المتعلقة بالموظفين الداخليين للمؤسسة يجب أن تخضع المؤسسة الموظفين الخارجيين لعمليات اللإشراف والرقابة وفيود الوصول المماثلة لذلك التي يتم تنفيذها للموظفين. للمساءلة وتحديد الوصول غير المخول يجب التأكد من أن سجلات وصول المستخدم تم تحديدها بشكل منفرد وتسجيلها لأغراض التدقيق والمُراجعة.
- يجب على المؤسسة إجراء مراجعات منتظمة لامتيازات الوصول للمستخدم للتحقق من منح الامتيازات بشكل مناسب بحسب مبدأ "الأقل امتياز. قد تسهل العملية تحديد الحسابات الساكنة والزائدة عن الحاجة، فضلا عن الكشف عن الوصول الخاطئ.
- تمثل كلمات المرور خط الحماية الأول وإذا لم يتم تنفيذها بشكل مناسب فيمكن أن تكون الحلقة الأضعف في المؤسسة ومن ثم يجب أن تفرض المؤسسات رقابة قوية على كلمات المرور لوصول المستخدمين إلى التطبيقات والأنظمة وأن تتضمن عمليات الرقابة على كلمات المرور تغيير كلمة المرور عند تسجيل الدخول لأول مرة والحد الأدنى لطول كلمة المرور والتاريخ وتعقيد كلمة المرور، فضلاً عن مدة الصلاحية وكذلك تحديد الأوقات في اليوم التي يكون خلالها الدخول مسموحاً.

- يجب أن تتأكد المؤسسة من عدم الوصول لأي شخص إلى كل من أنظمة الإنتاج وأنظمة النسخ بشكل متزامن، ولا سيما ملفات البيانات ومرافق الحواسيب وأن أي شخص يحتاج إلى الوصول إلى ملفات النسخ الاحتياطي أو موارد استرداد النظام يجب أن يكون مخولا بحسب الأصول، وأن تمنح المؤسسة الوصول فقط الأعراض محددة ولمدة محددة.
- يجب على المؤسسة متابعة آخر المستجدات التقنية في مجال التعرف على المستخدمين ومنحهم صلاحيات الوصول والعمل على إدخالها بصفي أساليب بديلة عن كلمات المرور، ومنها تقنيات بصمة الأصبع وبصمة العين.

إدارة وصول الإمتيازات:

- يعتمد أمن المعلومات، في نهاية المطاف، الثقة بمجموعة صغيرة من الموظفين المهرة الذين يجب أن يخضعوا لضوابط ورقابة مُناسبة، وأن يكون من واجباتهم الوصول إلى موارد النظام تحت تدقيق دقيق، ويجب وضع معايير اختيار صارمة وفحص شامل عند تعيين الموظفين في العمليات الحرجة ووظائف الأمن.
- بعض التكتيكات الشائعة المستخدمة من قبل الخبراء في تخريب العمليات تشمل زرع قنابل منطقية، وتركيب نصوص خفية، وإنشاء نظام خلفي للحصول على الوصول غير المخول واكتشاف كلمات المرور وتخريبها، ومسؤولي النظام وموظفي أمن تقنية المعلومات والاتصالات والمبرمجين الذين يقومون بعمليات حرجة ويمتلكون القدرة على الحاق ضرر شديد بالنظم الحساسة التي يحتفظون بها أو يعملون بحكم وظائفهم المميزة والقدرة على الوصول إلى الامتيازات.
- ينبغي أن تشرف المؤسسة عن كتب على الموظفين الذين لديهم صلاحيات تحويل مرتفعة للوصول إلى النظام وأن يتم تسجيل جميع نشاطاتهم ومراجعتها؛ لأن لديهم المعرفة والموارد اللازمة التي قد تستخدم أو تسهل التحايل على أنظمة الرقابة والإجراءات الأمنية، ومن خلال تطبيق إجرءات الرقابة والممارسات الأمنية الآتية:
  - تنفيذ اليات تصديق قوية، مثل التصديق ذي العوامل الثنائية للمستخدمين ذوي الامتيازات.
  - إنشاء إجراءات رقابة قوية على الوصول عن بعد بوساطة المستخدمين ذوي الامتيازات.
  - تقييد عدد المستخدمين ذوي الامتيازات.
  - منح الوصول إلى الامتيازات بحسب مبدأ "الحاجة".
  - الحفاظ على سجلات التدقيق لنشاطات النظام التي يقوم بها المستخدمون ذوو الامتيازات.

- عدم السماح للمستخدمين ذوي الامتيازات بالوصول إلى سجلات النظام التي يتم فيها النقاط نشاطاته.
- مراجعة نشاطات المستخدمين ذوي الامتيازات في الوقت المُناسب.
- حظر مشاركة حسابات الامتيازات.
- منع المزودين والمتعاقدين من الحصول على امتيازات الوصول إلى الأنظمة من دون عمليات الإشراف والرقابة عن كثب.
- حماية بيانات النسخ الاحتياطية من الوصول غير المصرح به.

السادس عشر: الخدمات المالية عبر الإنترنت:

- في حين يُقدم الإنترنت فُرصاً للمؤسسة للوصول إلى أسواق جديدة وتوسيع نطاق مُنتجاتها وخدماتها، لكونه شبكة مفتوحة، فإنه يجلب أيضاً مخاطر أمنية أكثر تطوراً وديناميكية من الشبكات المغلقة وقنوات التوصيل الخاصة؛ لذلك يجب أن تكون المؤسسة على دراية بالمخاطر التي تنشأ نتيجة تقديم الخدمات المالية عبر الإنترنت. هناك درجات متفاوتة من المخاطر المرتبطة بأنواع الخدمات المقدمة عبر الإنترنت عادة يمكن تصنيف الخدمات المالية المقدمة عبر الإنترنت إلى خدمات المعلومات وخدمة تبادل المعلومات التفاعلية وخدمة المعاملات وترتبط مستويات المخاطر المرتفعة مع خدمة المعاملات؛ لأن المعاملات عبر الإنترنت عادة ما تكون غير قابلة للإلغاء بمجرد أن يتم تنفيذها.
- يجب أن تُحدد المؤسسة بوضوح المخاطر المُرتبطة بأنواع الخدمات المقدمة في عملية إدارة المخاطر ويجب على المؤسسة أيضا وضع ضوابط أمنية، وعمليات توافرية النظام، وقدرات عمليات التعافي، التي تتناسب مع مستوى التعرض للمخاطر، لجميع عمليات الإنترنت.

حماية الأنظمة المرتبطة بالإنترنت:

- قد تستهدف الهجمات أنظمة المؤسسة المرتبطة بالإنترنت إذ يتم تقديم الخدمات المالية بشكل متزايد عبر الإنترنت وزيادة الزبائن والمتعاملين، وفي إجراء مضاد، يجب على المؤسسة وضع استراتيجية امنية، ووضع إجراءات لضمان سرية البيانات والأنظمة وتكاملها وتوافرها.
- يجب تزويد الزبائن والمستخدمين لخدمات الإنترنت بالتأكيدات بأن الوصول إلى الإنترنت والمعاملات التي تتم عبر الإنترنت على موقع المؤسسة الإلكتروني محمية وموثوقة بشكل كاف.

- يجب أن تقوم المؤسسات بتقييم المتطلبات الأمنية المرتبطة بأنظمة الإنترنت بشكل صحيح وتبني خوارزميات التشفير المعدة بحسب المعايير الدولية وتخضع للفحص الدقيق من قبل المجتمع الدولي لكاتبي التشفير أو معتمدة من قبل هيئات مهنية معتمدة أو وكالات حكومية.
- يجب تخزين ومعالجة ونقل المعلومات بين المؤسسة والزبائن بشكل كامل وموثوق ودقيق ومع اتصال الإنترنت بالشبكات الداخلية يمكن لأي شخص من أي مكان وفي أي وقت الوصول إلى الأنظمة والأجهزة. يجب تنفيذ إجراءات الحماية المادية والمنطقية للسماح للموظفين المخولين فقط بالوصول إلى الأنظمة.
- يجب على المؤسسة تثبيت أنظمة المراقبة بحيث يتم تنبيهها على أي نشاطات غير طبيعية في النظام، أو أخطاء في النقل، أو معاملات استثنائية عبر الإنترنت ويجب على المؤسسة إنشاء عملية متابعة للتحقق من أن هذه القضايا أو الأخطاء يتم تناولها بشكل مناسب في وقت لاحق.
- يجب أن تحافظ المؤسسة على مرونة عالية وتوافر للأنظمة عبر الإنترنت وأنظمة الدعم (مثل أنظمة الواجهة وأنظمة الاستضافة الخلفية وأجهزة الشبكة ويجب أن تضع المؤسسة تدابير لتخطيط الانتفاع وتتبعه، فضلا عن الحماية ضد الهجمات عبر الإنترنت. قد تتضمن هذه الهجمات الحرمان من الخدمة (DoS) وهجمات الحرمان من الخدمة الموزعة (DDoS).
- يجب أن تقوم المؤسسات المصرفية بتنفيذ عمليات التصديق ذات العوامل الثنائية عند تسجيل الدخول لجميع أنواع الأنظمة المالية من خلال الإنترنت وتوقيع المعاملة من أجل عمليات التخويل. وتتمثل الأهداف الرئيسة التصديق ذي العوامل الثنائية وتوقيع المعاملة إلى تأمين عملية تصديق الزبائن، وحماية سلامة بيانات حساب العميل وتفاصيل المعاملات، وكذلك لتعزيز الثقة في الأنظمة من خلال مكافحة الهجمات اللإلكترونية التي تستهدف المؤسسات المصرفية وزبائنها.
- فيما يخص المؤسسات المالية التي تقدم أنظمتها المالية عبر الإنترنت لتخدم المستثمرين المؤسسيين والمستثمرين المفوضين أو الشركات، إذ يتم تنفيذ عمليات الرقابة البديلة من أجل عمليات التفويض، يجب على المؤسسة إجراء تقييم للمخاطر على هذه الأنظمة لضمان مستوى الأمان لهذه الضوابط والعمليات.
- يجب اتخاذ الإجراءات المناسبة لتقليل التعرض لأنواع أخرى من الهجمات الإلكترونية، مثل الهجوم الوسيط الذي يُعرف أكثر باسم هجوم الوسيط (MITM)، أو هجوم الرجل في المتصفح، أو هجوم الرجل في التطبيق.

- مع دخول المزيد من الزبائن إلى المواقع الإلكترونية للمؤسسات للوصول إلى حساباتهم وإجراء مجموعة واسعة من المعاملات المالية لأغراض شخصية ولأغراض تجارية، يجب على المؤسسة وضع إجراءات لحماية الزبائن الذين يستخدمون الأنظمة الموصولة بالإنترنت، فضلا عن ذلك فستقوم المؤسسات التعليمية بتثقيف الزبائن بشأن الإجراءات الأمنية التي تضعها المؤسسة لحماية الزبائن في بيئات الإنترنت. يجب على المؤسسات ضمان حصول زبائنها على التثقيف المستمر لزيادة الوعي الأمني للزبائن

أمن خدمات الدفع الإلكتروني وخدمات الإنترنت عبر الهاتف النقال:

- تشير خدمات الإنترنت عبر الهاتف النقال إلى توفير الخدمات المالية عبر الأجهزة المحمولة مثل الهواتف النقالة أو الأجهزة اللوحية. قد يختار الزبائن الوصول إلى هذه الخدمات المالية عبر متصفحات الويب على الهواتف الجوالة أو التطبيقات المطورة ذاتيا على منصات الهواتف النقالة مثل أنظمة تشغيل Google, Android Apple iOS, Microsoft, Windows .
- يشير الدفع بوساطة الهاتف النقال إلى استخدام الأجهزة لإجراء عمليات الدفع ويمكن إجراء هذه العمليات باستخدام.

تقنيات مختلفة مثل الاتصال على مستوى النطاق (NFC) .

- الخدمات وعمليات الدفع عبر الإنترنت هي امتداد للخدمات المالية وخدمات الدفع من خلال الإنترنت التي تقدمها المؤسسات المصرفية ويمكن الوصول إليها من الإنترنت عبر أجهزة الكمبيوتر أو أجهزة الكمبيوتر المحمولة ويجب على المؤسسة أيضا تطبيق إجراءات أمنية مماثلة لتلك التي تطبق على أنظمة الدفع المالي، والدفع من الإنترنت على خدمات المحمول عبر الإنترنت وأنظمة الدفع، ويجب أيضا إجراء تقييم للمخاطر لتحديد سيناريوهات الاحتيال المحتملة ووضع التدابير المناسبة لمواجهة عمليات احتيال بطاقات الدفع عبر الأجهزة المحمولة.
- نظرا إلى أن أجهزة الهاتف المحمول معرّضة للفقدان والسرقة فيجب على المؤسسة التأكد من وجود إجراءات الحماية الكافية للمعلومات الحساسة والسرية المستخدمة في الخدمات وعمليات الدفع من خلال الإنترنت ويجب أن يكون لدى المؤسسة معلومات حساسة أو سرية مشفرة لضمان سرية وسلامة هذه المعلومات في التخزين والنقل. وبمعالجتها في بيئة آمنة.
- يجب تثقيف الزبائن بشأن التدابير الأمنية لحماية أجهزتهم المحمولة من الفيروسات وغيرها من البرامج الخبيثة التي تُسبب أضراراً جسيمة ولها عواقب مؤذية.

- يجب حماية الأجهزة المرتبطة بأنظمة المدفوعات (ACH,RTGS) وخاصة الأجهزة الخاصة بنقل ملفات ال (STP)بين النظام المحاسبي الشامل وانظمة المدفوعات.

السابع عشر: أمن خدمات الدفع الإلكتروني (ماكينات الصرف الآلي، بطاقات الدائنون والمدينون:

- تُتيح بطاقات الدفع لحامِليها المُرونة في إجراء عمليات الشراء أينما كانوا، قد يختار حاملو البطاقات إجراء عمليات الشراء عن طريق تقديم هذه البطاقات فعليا للدفع لدى المتاجر، أو يمكنهم اختيار شراء حاجياتهم عن طريق الإنترنت او من خلال البريد أو الهاتف وتوافر بطاقات الدفع لحامليها سهولة سحب النقود في أجهزة الصرف الآلي ("ATM") أو في المتاجر.
- وتشمل أنواع الاحتيال في البطاقات على التزييف والضياع والسرقة وحالات عدم تسلم البطاقة (CNR)وحالات عدم عرض البطاقة (CNP) .

الاحتيالات المتعلقة ببطاقات الدفع:

- يجب على المؤسسة الذي تُقدم خدمات بطاقات الدفع أن تُقيم ضمانات كافية لحماية البيانات الحساسة لبطاقات الدفع. وينبغي التأكد من تشفير البيانات الحساسة للبطاقة لضمان سرية وسلامة هذه البيانات في التخزين والنقل، وتتم معالجة المعلومات السرية في بيئة آمنة.
- يجب على المؤسسة نشر رقائق أمنة لتخزين البيانات الحساسة للبطاقة. ويجب أيضا تنفيذ أساليب تصديق قوية للبطاقات، مثل أساليب تصديق البيانات الديناميكية ("DDA")، أو أساليب تصديق البيانات المدمجة ("CDA") العمليات البطاقات عبر الإنترنت أو من دون إنترنت. وفيما يخص المعاملات التي يُنفذها الزبائن ببطاقات الصراف الآلي الخاصة بهم، يجب أن تسمح المؤسسة فقط بتصريح المعاملات عبر الإنترنت، ويجب على جهة إصدار البطاقة وليس مقدم الخدمة معالجة عمليات الدفع للجهات الخارجية وإجراء التصديق على المعلومات الثابتة الحساسة للزبائن مثل أرقام التعريف الشخصية أو كلمات المروز. وينبغي إجراء مراجعات امنية منتظمة للبنية التحتية والعمليات التي يستخدمها زبائن مقدمي هذه الخدمة.
- يجب أن يتم تنفيذ ضوابط الأمان في أنظمة وشبكات بطاقات الدفع.
- يجب على المؤسسة إرسال بطاقات الدفع الفعالة الجديدة إلى العميل عبر البريد فقط بناءً على الضوابط أو تسليمها باليد وبشكل شخصي، بعد التأكد من هوية العميل.

- يجب تنفيذ كلمة مرور ديناميكية لمرة واحدة (OTP) لمعاملات عدم عرض البطاقة (CNP) عبر الإنترنت لتقليل مخاطر الاحتيال المرتبطة بعدم عرض البطاقة (CNP) .
- لتعزيز حماية بطاقات الدفع يجب على المؤسسة فورًا إبلاغ حاملي البطاقات من خلال التنبيهات عندما تتجاوز السحوبات الرسوم المحددة للعميل. وأن تتضمن هذه التنبيهات معلومات مثل المصدر وقيمة المعاملة.
- يجب على المؤسسة وضع انظمة كشف الاحتيال المتينة ذات الأهداف السلوكية أو ما يعادلها وقدرات الترابط لتحديد ومنع النشاطات الاحتيالية ويجب أن تحيد مقابيس إدارة المخاطر وفقا للمخاطر التي يتعرض لها حاملو البطاقات أو طبيعة المعاملات أو عوامل الخطر الأخرى لتعزيز قدرات كشف الاحتيال.
- يجب على المؤسسة متابعة العمليات التي تظهر انحرافا كبيرًا عن سلوك استخدام البطاقة المعتاد لحامل البطاقة. ويجب التحقيق في هذه المعاملات والحصول على موافقة حامل البطاقة قبل إكمال المعاملة.

حماية أجهزة الصراف الآلي وأكشاك الدفع:

- بوافر وجود اجهزة الصراف الآلي وأكشاك الدفع على سبيل المثال، (أجهزة SAM وAXS)، لحاملي البطاقات سهولة سحب النقود وعمليات سداد الفواتير، ومع ذلك فإن هذه الأنظمة هي أهداف إذ يتم تنفيذ هجمات التزوير للبطاقات.
- ولضمان ثقة المستخدم في استخدام هذه الأنظمة ينبغي وضع التدابير الآتية للتصدي لهجمات الاحتيال على أجهزة الصراف الآلي وأكشاك الدفع.
- تثبيت حلول لمكافحة التزوير على هذه الأجهزة والأكشاك للكشف عن وجود الأجهزة الغريبة الموضوعة فوق أو بالقرب من فتحة إدخال البطاقة.
- تثبيت آليات الكشف وإنذار الموظفين المناسبين المؤسسة لمتابعة الاستجابة والقيام بالتصرف المُناسب.
- تنفيذ لوحات مفاتيح مقاومة للتزوير لضمان تشفير رموز PIN الخاصة بالزبائن أثناء العملية.
- تنفيذ التدابير المناسبة لمنع تصفح الرمز السري PIN للعميل.

- إجراء المراقبة بالفيديو للنشاطات التي تتم في هذه الأجهزة والأكشاك والحفاظ على جودة التسجيلات. ويجب أن تَتَحَقَّق المؤسسة من تنفيذ إجراءات الأمان المادية المُناسبة في أكشاك الدفع الخاصة بالشركات الأخرى التي تقبل بطاقات دفع المؤسسة وتُعَالِجُها.

المُرفقات

مرفق رقم (1)

مصفوفة الأهداف المؤسسية

01	تحقيق القيمة المضافة من أصول وإستثمارات المؤسسة	• نسبة الأصول والإستثمارات التي حققت توقعات ذوي المصلحة بشأن القيمة المضافة • نسبة المنتجات والخدمات التي حققت المنافع المرجوة منها • نسبة الإستثمارات التي حققت المنافع المرجوة منها
02	محفظة من الخدمات والمنتجات التنافسية	• نسبة المنتجات والخدمات التي حققت أو تجاوزت المتوقع من الأهداف والعوائد والحصة في السوق • نسبة المنتجات والخدمات التي حققت رضا الزبائن • نسبة المنتجات والخدمات التي حققت ميزة تنافسية في السوق
03	إدارة والمخاطر الكلية المؤسسية (حماية الأصول)	• نسبة الأهداف والخدمات الرئيسة المشمولة بعمليات تقييم المخاطر • عدد الحوادث الرئيسة غير المحددة ضمن عمليات تقييم المخاطر من مجموع الحوادث الكلي • تحديث دوري لملف المخاطر
04	الإمتثال للقوانين والضوابط	• كلفة عدم الإمتثال للقوانين والضوابط بما يشمل الغرامات والتسويات • عدد الموضوعات المخالفة للقوانين والضوابط التي سببت رأياً عاماً تجاه المؤسسة أو سمعة سيئة • عدد الموضوعات المخالفة لشروط التعاقد مع الغير
05	الإفصاح والشفافية المالية	• نسبة الأصول والإستثمارات التي تم تحديدها والموافقة على موازناتها وعوائدها المتوقعة • نسبة تكاليف الخدمات الممكن توزيعها على المستخدمين • نسبة الرضا التي حققت المتوقع من قبل ذوي المصلحة فيما يخص الشفافية المالية، والدقة والفهم للبيانات المالية
06	ثقافة مؤسسية خدمية موجهة للزبائن	• عدد حوادث الإنقطاع للخدمات المصرفية والمالية بسبب حودات متعلقة بتقنية المعلومات والإتصالات • نسبة رضا ذوي المصلحة على الخدمات والمنتجات المقدمة • عدد شكاوي الزبائن

مرفق رقم (1)

مصفوفة الأهداف المؤسسية (Enterprise goals)

70	إستمرارية الخدمات وتوافرها	• عدد حوادث توقف الخدمات الرئيسة والحرجة • تكاليف حوادث توقف العمليات والخدمات • عدد ساعات توقف العمليات والخدمات • نسبة الشكاوي المُتعلقة بتوقف العمليات والخدمات
80	سرعة التغيير إستجابة لمتطلبات بيئة العمل	• مستوى رضا المجلس عن سرعة الاستجابة للمتطلبات الجديدة • عدد الخدمات والمنتجات المُقدمة من عمليات جديدة مستحدثة • متوسط الزمن المستغرق للبدء بتحقيق أهداف إستراتيجية موافق عليها
90	منهجية لصنع قرار مبني على المعلومات	• درجة رضا المجلس والإدارة التنفيذية العليا على عمليات صنع القرار • عدد الحوادث الناتجة عن قرارات خاطئة بسبب الإرتكاز على معلومات غير دقيقة • الزمن المستغرق لتوفير المعلومات اللازمة لصنع القرار
10	تقليل تكاليف الخدمات والمنتجات	• الإتجاه الزمني للتكاليف بالمقارنة مع مستوى الخدمات • تقييم دوري لتكاليف الخدمات المُقدمة • مستوى رضا المجلس و الإدارة التنفيذية العليا تجاه تكاليف الخدمات المُقدمة
11	تحسين مستوى الخدمات المُقدمة	• تقييم دوري لمستوى النضوج للخدمات المُقدمة • نتائج وإتجاه التقييم لمستوى النضوج • رضا المجلس و الإدارة التنفيذية العليا على كفاءة عمليات المؤسسة
12	تقليل تكاليف عمليات المؤسسة	• تقييم دوري لتقليل تكاليف العمليات • الإتجاه الزمني للتكاليف بالمقارنة مع مستوى الخدمات • مستوى رضا المجلس و الإدارة التنفيذية العليا على تكاليف العمليات

مرفق رقم (1)

مصفوفة الأهداف المؤسسية (Enterprise goals)

13	إدارة برامج التغيير للأعمال	• عدد البرامج المنجزة في الوقت المخطط له والموازنات المقدرة مسبقاً • نسبة رضا ذوي المصالح عن البرامج المنجزة البرامج المنجزة • نسبة المعرفة والوعي بتغييرات الأعمال نتيجة لمبادرات تقنية المعلومات والإتصالات
14	إنتاجية تشغيلية وعمالية	• عدد البرامج / المشاريع المنجزة بالوقت وبالموازنات المرصودة • مستويات التكاليف والعمالة المشغلة مقارنة بالمستهدفات
15	الأمتثال للسياسات الداخلية	• عدد الحوادث الناتجة بسبب عدم الامتثال للسياسات الداخلية • نسبة ذوي المصلحة وذوي المعرفة والوعي بالسياسات الداخلية • نسبة السياسات المُفعلة في المؤسسة
16	موظفون ذوو مهارة	• مستوى رضا ذوي المصلحة عن خبرات ومهارات الموظفين • نسبة الوظائف المشغولة بأقل من المهارات والخبرات والمعارف المطلوبة • مستوى الرضى الوظيفي
17	ثقافة تميز وإبداع	• مستوى المعرفة والوعي بفرص الإبداع والتميز • رضا ذوي المصلحة تجاه مستوى التميز والإبداع والأفكار المطروحة • عدد المنتجات والخدمات المطروحة والموافق عليها والناتجة عن مبادرات ومقترحات إبداعية

مرفق رقم (2)

مصفوفة أهداف المعلومات والتقنية المصاحبة لها (information and related technology goals)

رمز الهدف	الأهداف	معايير قياس وتحقيق الأهداف	أرقام الأهداف المؤسسة ذات الصلة المباشرة
01	توافق الخطة الإستراتيجية لتقنية المعلومات مع الخطة الأاستراتيجية للمؤسسة، من خلال إتباع منهجية لصنع القرار الإستراتيجي للمؤسسة، كفوءة وتلبي متطلبات بيئة العمل الداخلية والخارجية	• نسبة أهداف المؤسسة الإستراتيجية المدعومة بأهداف تقنية المعلومات والإتصالات الإستراتيجة • مستوى الرضا من قبل وحدات المؤسسة على محفظة المشاريع والخدمات المخطط لتنفيدها ومدى تحقيقها للمتطلبات بكفاءة وفعالية، ويمكن قياسه من خلال إتباع أسلوب الأستبيان على سبيل المثال لا الحصر	01,03,05,07,11,13
02	إمتثال ممارسات تقنية المعلومات والاتصالات ومساهمتها في امتثال المؤسسة للقوانين والأنظمة والضوابط المرعية	• تكلفة عدم إمتثال تقنية المعلومات والاتصالات بما في ذلك تكاليف التصحيح المطلوبة، فضلاً عن مدى التأثير في سمعة المؤسسة بهذا الشان • عدد ملحوظات عدم الأمتثال لمتطلبات تقنية المعلومات والاتصالات المرفوعة لمجلس الإدارة أو تلك التي تثير الرأي العام بشأنها	01,05,07,09,12,17
03	الإلتزام من قبل الأغدارة بإتخاذ قرارات مبنية على معطيات تقنية المعلومات والاتصالات	• نسبة المهام والواجبات المتعلقة بتقنية المعلومات والاتصالات من إجمالي المهام والواجبات للوصف الوظيفي لوظائف المؤسسة • عدد المرات التي يتم فيها مناقشة موضوعات متعلقة بتقنية المعلومات والاتصالات في إجتماعات مجلس الإدارة • إجتماعات دورية ومنتظمة للجنة حوكمة تقنية المعلومات والاتصالات، واللجنة التوجيهية لتقنية المعلومات والاتصالات	04,10,16
04	إدارة مخاطر تقنية المعلومات والاتصالات لعمليات المؤسسة	• نسبة عمليات المؤسسة الحساسة المرتكزة على الموارد والبنية التحتية لتقنية المعلومات والأتصالات والمشمولة ضمن عمليات تقييم المخاطر • عدد حوادث تقنية المعلومات والاتصالات الرئيسة التي لم تؤخذ بالحسبان لدى تقييم المخاطر • نسبة العمليات التي تحتوي مخاطر تقنية المعلومات والاتصالات إلى مجموع العمليات المشمولة ضمن تقييم المخاطر • دورية تحديث ملف المخاطر (Risk profile)	02,10

مرفق رقم (2)

مصفوفة أهداف المعلومات والتقنية المصاحبة لها (information and related technology goals)

رمز الهدف	الأهداف	معايير قياس وتحقيق الأهداف	أرقام الأهداف المؤسسة ذات الصلة المباشرة
05	ضمان تحقيق المنفعة والقيمة المضافة من محفظة موارد تقنية المعلومات والإتصالات ومشاريعها وخدماتها	• نسبة مشاريع تقنية المعلومات والإتصالات التي تم فيها مراقبة وقياس المنافع والقيمة المضافة خلال مدة عمر المشروع • نسبة مشاريع تقنية المعلومات والإتصالات والخدمات التي حققت المنافع والنتائج المستهدفة وتلك التي تجاوزت المستهدفات	06
06	الشفافية في الإفصاح عن تكاليف تقنية المعلومات والإتصالات ومنافعها ومخاطرها	• نسبة المشاريع في المؤسسة التي تم فيها تحديد مصاريف تقنية المعلومات والإتصالات ونتائجها المتوقعة، والموافقة عليها • مستوى الرضا المسموح به عن مستوى الإفصاح والفهم والدقة للمخصصات المالية للمشاريع وخدمات تقنية المعلومات والإتصالات	01,07
07	تقديم خدمات تقنية المعلومات والإتصالات التي تلبي متطلبات عمليات المؤسسة	• عدد مرات توقف عمليات المؤسسة بسبب حوادث وانقطاع خدمات تقنية المعلومات والإتصالات • مستوى الرضا من قبل أقسام المؤسسة على قيام إدارة تقنية المعلومات والإتصالات بتحقيق متطلبات العمل في الوقت والمواصفات المتفق عليها ضمن اتفاقيات مستوى الخدمات الخارجية والداخلية	04,10,14
08	الإستخدام المناسب للبرمجيات وحلول تقنية المعلومات والإتصالات	• نسبة مسؤولي عمليات المؤسسة الراضيين عن منتجات وخدمات تقنية المعلومات والإتصالات • مستوى فهم مسؤولي عمليات المؤسسة لخصائص البرمجيات وحلول تقنية المعلومات والإتصالات على دعم عملياتهم • مستوى الرضا عن التدريب المقدم لمستخدمي تقنية المعلومات والإتصالات وعن مدى كفاية دليل إستخدام البرمجيات والحلول المختلفة	01,07,09,17
09	رشاقة عمليات تقنية المعلومات والإتصالات وإدارة مواردها	• مستوى رضا مسؤولي المؤسسة على مستوى الاستجابة لمتطلباتهم من تقنية المعلومات والإتصالات	01,14

		• عدد عمليات المؤسسة المخدومة من قبل موارد حديثة لتقنية المعلومات والإتصالات • الوقت المتوسط المستغرق لترجمة الهدف الاستراتيجي لمفردات مبادرة تقنية المعلومات والإتصالات	
10	أمن المعلومات، تشغيل البرمجيات والبنية التحتية لتقنية المعلومات والإتصالات	• عدد حوادث أمن المعلومات التي تسببت بخسائر مالية أو إنقطاع في العمليات أو التأثير في السمعة • عدد خدمات تقنية المعلومات والإتصالات المُحددة فيها المتطلبات الأمنية لتقنية المعلومات والإتصالات • المدة الزمنية اللازمة لإجراء التعديلات المطلوبة على مستوى إمتيازات النفاذ للمستخدمين • تقييم دوري لمعطيات أمن المعلومات بحسب أحدث المعايير الدولية المقبولة	04,06,11

مصفوفة أهداف المعلومات والتقنية المصاحبة لها (Alignment Goals)

رمز الهدف	الأهداف	معايير قياس وتحقيق الأهداف	أرقام الأهداف المؤسسة ذات الصلة المباشرة
11	الإستغلال الأمثل لموارد وقدرات تقنية المعلومات والإتصالات	• تقييم دوري لدرجة النضوج وتكاليف موارد تقنية المعلومات والإتصالات • نتائج واتجاه التقييم أعلاه • مستوى الرضا من قبل إدارة المؤسسة ككل على قدرات تقنية المعلومات والإتصالات وعلى حجم التكاليف	01,07,08,09,12
12	دعم أليات العمل من خلال تكامل البرمجيات التطبيقية وموارد التقنية ضمن عمليات المؤسسة	• عدد الحوادث الناتجة بسبب أخطاء تكامل البرمجيات • عدد حوادث تعطل عمليات المؤسسة بسبب تعطل برمجيات و تقنية المعلومات والإتصالات • عدد مرات تعطل مشاريع أو تأخرها بسبب البنية التحتية ومشاكل تقنية المعلومات والإتصالات • عدد البر مجيات والحلول غير المتكاملة، والتي تعمل بمعزل عن باقي البرمجيات والحلول	05,06,11
13	تنفيذ المشاريع ضمن الزمن والموازنات المالية المحددة مسبقاً ضمن إطار إدارة محفظة للمشاريع تتوافق والقواعد والمعايير الدولية المتبعة بهذا الشأن	• عدد المشاريع المنفذة ضمن حدود الزمن والموازنة المرصودة • نسبة الرضا من قبل ذوي المصلحة عن جودة إدارة المشاريع • عدد المشاريع التي تتطلب إعادة بسبب ضعف الجودة في الأداء وتحقيق الأهداف • نسبة تكاليف الصيانة إلى إجمالي تكاليف تقنية المعلومات والإتصالات	01,03,13
14	توافرية معلومات معتمد عليها ومفيدة مرتكز عليها في إتخاذ القرار	• مستوى رضا دوائر المؤسسة على جودة المعلومات وتوافريتها • عدد حوادث عمليات المؤسسة بسبب قلة توافرية المعلومات والتقنية • نسبة أهمية قرارات المؤسسة الخاطئة بسبب قلة توافرية المعلومات والتقنية	
15	إمتثال ممارسات تقنية المعلومات والإتصالات للسياسات الداخلية للمؤسسة	• عدد حوادث تقنية المعلومات والإتصالات نتيجة عدم الإمتثال للسياسات • نسبة الأفراد ذوي الفهم الصحيح للسياسات • نسبة السياسات التي تحاكي أفضل الممارسات الدولية	

		• دورية مراجعة وتحديث السياسات	
16	مستوى المهارات والتنافسية لكوادر المؤسسة بشكل عام وكوادر تقنية المعلومات والإتصالات	• نسبة الموظفين الذين لديهم مهارات تقنية معلومات كافية لمتطلبات العمل • نسبة رضا الموظفين للمهام المتعلقة بتقنية المعلومات والإتصالات المنوطة بهم • عدد ساعات التدريب والتعلم للموظف	
17	امتلاك المعرفة والخبرة في الإبتكارات التقنية الممكن توفيرها لتطوير عمليات المؤسسة	• مستوى المعرفة في عمليات المؤسسة والإبتكارات التقنية الممكن توفيرها لدعم تلك العمليات	

مرفق رقم (3)

عمليات حوكمة تكنولوجيا المعلومات والإتصالات وأهداف الحوكمة والإدارة (Governance and Management Objectives)

رمز العملية	عنوان العملية	وصف العملية	هدف العملية	أرقام وأهداف المعلومات والتقنية المصاحبة لها ذات الصلة المباشرة
عمليات التقييم والتوجيه والرقابة				
EDM 01	ضمان إعداد الإطار العام لحوكمة تكنولوجيا المعلومات والإتصالات وتحديثه	تحليل وتوضيح متطلبات حوكمة تكنولوجيا المعلومات والإتصالات ووضع سياسات عمل تقنية المعلومات والإتصالات ومبادئه وإجراءاته، والهياكل التنظيمية ذات العلاقة، والإستمرار بتطويرها وتحديثها مع تحديد واضح للمسؤليات والصلاحيات الكفيلة بتحقيق أهداف المؤسسة	إيجاد منهجية متكاملة تتوافق والإطار العام للحوكمة المؤسسية، لضمان أخذ قرارات تقنية المعلومات والإتصالات تتماشى مع تحقيق الأهداف الإستراتيجية للمؤسسة، وأن عمليات تقنية المعلومات والإتصالات مراقبة بكفاءة وشفافية عاليتين ضمن إطار الإمتثال لإستراتيجية المؤسسة وسياساتها والضوابط والأنظمة والقوانين المراعاة بهذا الشأن	01,03,07
EDM 02	ضمان تحقق المنافع وتوصيلها	تعظيم القيمة المضافة من خلال عمليات المؤسسة وموارد تقنية المعلومات والإتصالات الموظفة بكلف مقبولة	الإستغلال الأمثل وتعظيم حجم المنافع من موارد تقنية المعلومات والإتصالات بأقل التكاليف الممكنة بما يلبي ويحقق متطلبات العمل	01,05,06,07,17
EDM 03	ضمان إدارة صحيحة لمخاطر تقنية المعلومات والإتصالات	الفهم السليم للمخاطر من حيث القابلية على تحمل المخاطر (Risk appetite) ودرجة تحمل المخاطر (Risk tolerance)، وتبرير القيمة المضافة، والمنافع من وراء قبول تلك المخاطر، فضلاً عن توضيح وتوثيق وتوصيل تلك القواعد لذوي العلاقة	ضمان عدم تجاوز مخاطر تقنية المعلومات والإتصالات من حيث قابلية تحملها المخاطر المحددتين، وضمان تحديد وإدارة مخاطر تقنية المعلومات والإتصالات وتقليل إحتمالية مخالفة القوانين والأنظمة والضوابط	04,06,10,15
EDM 04	ضمان الإستغلال الأمثل لموارد تقنية المعلومات والإتصالات	ضمان ملاءة وتوافر موارد العمليات وتقنية المعلومات والإتصالات (العنصر البشري، وإجراءات العمل، والتقنية) لتلبية أهداف المؤسسة بكفاءة، بأقل الكلف الممكنة	ضمان الإستغلال الأمثل للموارد بما في ذلك موارد تقنية المعلومات والإتصالات، وأن هناك زيادة محتملة في المنافع المحققة	09,11,16

مرفق رقم (3)

عمليات وأهداف الحوكمة والإدارة (Governance and Management Objectives)

رمز العملية	عنوان العملية	وصف العملية	هدف العملية	أرقام وأهداف المعلومات والتقنية المصاحبة لها ذات الصلة المباشرة
EDM 05	ضمان الشفافية والإفصاح لذوي المصلحة	ضمان الشفافية في العمليات والتقارير الخاصة بتقييم أداء إدارة تقنية المعلومات والإتصالات، والتأكد من تحديد والموافقة على الأهداف والمعايير الخاصة بالإجراءات التصحيحية بهذا الشأن	التأكد من وصول تقارير قياس الاداء لموارد تقنية المعلومات والإتصالات لذوي العلاقة في الوقت اللازم، بهدف تحسين مستوى الأداء، وتحديد المواضيع التي تكون بحاجة إلى تحسين وعناية، والتأكد من أهداف تقنية المعلومات والإتصالات تتماشى والأهداف الإستراتيجية للمؤسسة	03,06,07
عمليات التو افق والتخطيط والتنظيم (APO) Align , plan and Orgnize				
APO 01	تفعيل الإطار العام لإدارة تقنية المعلومات والإتصالات	التوضيح والإستمرار بتحديث الرؤية والرسالة بشان حوكمة تكنولوجيا المعلومات والإتصالات، والإستمرار في توظيف آليات العمل وتفويض الصلاحيات اللازمة لإدارة المعلومات بإستخدام تقنيات لتحقيق أهداف المؤسسة ضمن إطار الإلتزام بالمبادئ والسياسات	إستخدام منهجية إدارية متناسقة لتحقيق متطلبات حوكمة تكنولوجيا المعلومات والإتصالات تشمل كل من الهياكل التنظيمية المطلوبة،والأدوار والمسؤوليات والنشاطات والعمليات،والمهارات والخبرات	01,02,09,11,15,16,17
APO 02	إدارة الإستراتيجية Manage strategy	تقديم وصف كامل للوضع الحالي للمؤسسة ولبيئة تقنية المعلومات والإتصالات وتحديد التوجه المستقبلي متضمناً المبادرات المطلوبة للإنتقال لبيئة العمل المستقبلية، وتوظيف موارد وقدرات المؤسسة والخدمات المقدمة والمستعان بها من قبل الغير بفعالية وإعتمادية عاليتين لتحقيق الاهداف الإستراتيجة للمؤسسة	مواءمة الأهداف الإستراتيجية لتقنية المعلومات والإتصالات لتلبية تحقيق أهداف المؤسسة، وتحديد المسؤوليات تجاه تحقيق الأهداف بوضوح، والتأكد من الفهم الصحيح لها من قبل ذوي المصلحة	01,07,17

مرفق رقم (3)

عمليات وأهداف الحوكمة والإدارة (Governance and Management Objectives)

رمز العملية	عنوان العملية	وصف العملية	هدف العملية	أرقام وأهداف المعلومات والتقنية المصاحبة لها ذات الصلة المباشرة
EDM 05	ضمان الشفافية والإفصاح لذوي المصلحة	ضمان الشفافية في العمليات والتقارير الخاصة بتقييم أداء إدارة تقنية المعلومات والإتصالات، والتأكد من تحديد والموافقة على الأهداف والمعايير الخاصة بالإجراءات التصحيحية بهذا الشأن	التأكد من وصول تقارير قياس الاداء لموارد تقنية المعلومات والإتصالات لذوي العلاقة في الوقت اللازم، بهدف تحسين مستوى الأداء، وتحديد المواضيع التي تكون بحاجة إلى تحسين وعناية، والتأكد من أهداف تقنية المعلومات والإتصالات تتماشى والأهداف الإستراتيجية للمؤسسة	03,06,07
APO 01	تفعيل الإطار العام لإدارة تقنية المعلومات والإتصالات	التوضيح والإستمرار بتحديث الرؤية والرسالة بشان حوكمة تكنولوجيا المعلومات والإتصالات، والإستمرار في توظيف آليات العمل وتفويض الصلاحيات اللازمة لإدارة المعلومات بإستخدام تقنيات لتحقيق أهداف المؤسسة ضمن إطار الإلتزام بالمبادئ والسياسات	إستخدام منهجية إدارية متناسقة لتحقيق متطلبات حوكمة تقنية المعلومات والإتصالات تشمل كل من الهياكل التنظيمية المطلوبة،والأدوار والمسؤوليات والنشاطات والعمليات،والمهارات والخبرات	01,02,09,11,15,16,17
APO 02	إدارة الإستراتيجية Manage strategy	تقديم وصف كامل للوضع الحالي للمؤسسة ولبيئة تقنية المعلومات والإتصالات وتحديد التوجه المستقبلي متضمناً المبادرات المطلوبة للإنتقال لبيئة العمل المستقبلية، وتوظيف موارد وقدرات المؤسسة والخدمات المقدمة والمستعان بها من قبل الغير بفعالية وإعتمادية عاليتين لتحقيق الاهداف الإستراتيجة للمؤسسة	مواءمة الأهداف الإستراتيجية لتقنية المعلومات والإتصالات لتلبية تحقيق أهداف المؤسسة، وتحديد المسؤوليات تجاه تحقيق الأهداف بوضوح، والتأكد من الفهم الصحيح لها من قبل ذوي المصلحة	01,07,17

مرفق رقم (3)

عمليات وأهداف الحوكمة والإدارة (Governance and Management Objectives)

رمز العملية	عنوان العملية	وصف العملية	هدف العملية	أرقام وأهداف المعلومات والتقنية المصاحبة لها ذات الصلة المباشرة
EDM 05	ضمان الشفافية والإفصاح لذوي المصلحة	ضمان الشفافية في العمليات والتقارير الخاصة بتقييم أداء إدارة تقنية المعلومات والإتصالات، والتأكد من تحديد والموافقة على الأهداف والمعايير الخاصة بالإجراءات التصحيحية بهذا الشأن	التأكد من وصول تقارير قياس الاداء لموارد تقنية المعلومات والإتصالات لذوي العلاقة في الوقت اللازم، بهدف تحسين مستوى الأداء، وتحديد المواضيع التي تكون بحاجة إلى تحسين وعناية، والتأكد من أهداف تقنية المعلومات والإتصالات تتماشى والأهداف الإستراتيجية للمؤسسة	03,06,07
APO 01	تفعيل الإطار العام لإدارة تقنية المعلومات والإتصالات	التوضيح والإستمرار بتحديث الرؤية والرسالة بشان حوكمة تكنولوجيا المعلومات والإتصالات، والإستمرار في توظيف آليات العمل وتفويض الصلاحيات اللازمة لإدارة المعلومات بإستخدام تقنيات لتحقيق أهداف المؤسسة ضمن إطار الإلتزام بالمبادئ والسياسات	إستخدام منهجية إدارية متناسقة لتحقيق متطلبات حوكمة تكنولوجيا المعلومات والإتصالات تشمل كل من الهياكل التنظيمية المطلوبة،والأدوار والمسؤوليات والنشاطات والعمليات،والمهارات والخبرات	01,02,09,11,15,16,17
APO 02	إدارة الإستراتيجية Manage strategy	تقديم وصف كامل للوضع الحالي للمؤسسة ولبيئة تقنية المعلومات والإتصالات وتحديد التوجه المستقبلي متضمناً المبادرات المطلوبة للإنتقال لبيئة العمل المستقبلية، وتوظيف موارد وقدرات المؤسسة والخدمات المقدمة والمستعان بها من قبل الغير بفعالية وإعتمادية عاليتين لتحقيق الاهداف الإستراتيجة للمؤسسة	مواءمة الأهداف الإستراتيجية لتقنية المعلومات والإتصالات لتلبية تحقيق أهداف المؤسسة، وتحديد المسؤوليات تجاه تحقيق الأهداف بوضوح، والتأكد من الفهم الصحيح لها من قبل ذوي المصلحة	01,07,17

مرفق رقم (3)

عمليات وأهداف الحوكمة والإدارة (Governance and Management Objectives)

رمز العملية	عنوان العملية	وصف العملية	هدف العملية	أرقام وأهداف المعلومات والتقنية المصاحبة لها ذات الصلة المباشرة
APO 03	إدارة هيكلية تقنية المعلومات والإتصالات Manage Enterprise Architecture	إنشاء الهيكل العام لإدارة تقنية المعلومات والإتصالات بما في ذلك عمليات المؤسسة والمعلومات والبيانات والبرامج والبنية التحتية لتقنية المعلومات والإتصالات بغرض تحقيق أهداف التقنية وأهداف المؤسسة الإستراتيجية بكفاءة وفعالية، من خلال إنشاء نماذج وممارسات عمل رئيسة، وتحديد المتطلبات اللازمة لغيجاد مجموعة من المبادئ والإجراءات والأداوات المترابطة مع بعضها البعض، والعمل على تحسين مستوى التوافق بين التقنية ومتطلبات عمل المؤسسة، وزيادة رشاقة خدمات تقنية المعلومات والإتصالات، وتحسين جودة المعلومات والتقنية المعتمد عليها في تسيير عمليات المؤسسة	تحديد المعطيات المختلفة اللازمة لبناء إدارة تقنية المعلومات والإتصالات، وتحديد المبادئ والإجراءات المستخدمة في ذلك وتوصيف العلاقات بينهما للوصول إلى الأهداف التشغيلية والإستراتيجية للمؤسسة	01,09,11
APO 04	إدارة الإبتكارات Manage Innovation	زيادة الوعي بما هو معروض من جديد في سوق تقنية المعلومات والإتصالات لدراسة إمكانية إستغلال ذلك لدعم عمليات المؤسسة الحالية والمبتكرة لخدمة تحقيق أهداف المؤسسة الإستراتيجة	تحقيق الميزة التنافسية للمؤسسة من خلال تطوير وزيادة كفاءة وفعالية عماليات المؤسسة إستناداً إلى جديد تقنية المعلومات والإتصالات	05,08,09,11,17

مرفق رقم (3)

عمليات وأهداف الحوكمة والإدارة (Governance and Management Objectives)

رمز العملية	عنوان العملية	وصف العملية	هدف العملية	أرقام وأهداف المعلومات والتقنية المصاحبة لها ذات الصلة المباشرة
APO 05	إدارة محفظة المشاريع Manage Project portfolio	تنفيذ مشاريع تقنية المعلومات والإتصالات المختلفة التي تلبي الأهداف والتوجه الإستراتيجي للمؤسسة، مع الأخذ بالحسبان محدودية الموارد ومن تم الإستغلال الأمثل لها، والعمل على تقييم وترتيب أولوية المشاريع وفقاً لمساهمتها في تحقيق الأهداف الإستراتيجة وعلى مستوى الفرص والمخاطر المقابلة لذلك، والعمل على توظيف منتجات المشاريع إلى آليات وأداوات تخدم عمليات المؤسسة، والإسترار بمراقبة المنافع ومستوى القيمة المضافة لمحفظة المشاريع وإجراء التعديلات اللازمة في حينه إستناداً إلى التغذية الراجعة من عمليات المراقبة تلك، وعلى التغييرات في خطة عمل المؤسسة	تعظيم الفائدة والإستغلال الأمثل للموارد من خلال إدارة شاملة جامعة لمحفظة مشاريع المؤسسة	01,05,13
APO 06	إدارة الموازنة والكلفة Manage budget cost	إدارة الشؤون المالية لموارد تقنية المعلومات والإتصالات من خلال آليات عمل كل من الإدارة المالية وإدارة تقنية المعلومات والإتصالات في المؤسسة، بما في ذلك إعداد الموازنات ودراسة الكلف والمنافع وترتيب أولويات من خلال إستخدام أسس ومعايير موضوعية موحدة معتمدة في المؤسسة بهذا الشأن، والعمل بالتشاور مع ذوي المصلحة بتعديل المخصصات المرصودة بما يخدم الأهداف الإستراتيجة والتكتيكية للمؤسسة	توطيد العلاقة المشتركة بين إدارة تقنية المعلومات والإتصالات وذوي المصلحة في المؤسسة لضمان الإستغلال الأمثل لموارد التقنية وتقديم المعلومات بهذا الشان بشفافية عالية تسهل عمليات المساءلة وتقدير حجم المنافع والقيمة المضافة، وتسهيل آليات إتخاذ القرار في توظيف موارد تقنية المعلومات والإتصالات	05,06

مرفق رقم (3)

عمليات وأهداف الحوكمة والإدارة (Governance and Management Objectives)

رمز العملية	عنوان العملية	وصف العملية	هدف العملية	أرقام وأهداف المعلومات والتقنية المصاحبة لها ذات الصلة المباشرة
APO 07	إدارة الموارد البشرية Manage human resources	توظيف منهجية تضمن إيجاد الهياكل التنظيمية وخطوط الإتصال المؤسسي الأفقي والعمودي، وتوظيف العنصر البشري الماهر والكفوء وتوزيع الصلاحيات والمهام والأدوار والمسؤوليات، وإيجاد خطط التدريب والتعلمالمستمر، وتحفيز الموظفين الموظفين بشكل دائم للحصول على الاداء المطلوب	الإستغلال الأمثل للموارد البشرية لخدمة أهداف المؤسسة	01,11,13,16,17
APO 08	إدارة العلاقات Manage relationship	التوضيح والإستمرار بتحديث الرؤية والرسالة بشان حوكمة تكنولوجيا المعلومات والإتصالات، والإستمرار في توظيف آليات العمل وتفويض الصلاحيات اللازمة لإدارة المعلومات بإستخدام تقنيات لتحقيق أهداف المؤسسة ضمن إطار الإلتزام بالمبادئ والسياسات	تحسين النتائج وزيادة مستوى الثقة والإعتماد الكفوء لموارد تقنية المعلومات والإتصالات	01,07,12,17
APO 09	إدارة إتفاقيات الخدمات Manage service agreements	تقديم وصف كامل للوضع الحالي للمؤسسة ولبيئة تقنية المعلومات والإتصالات وتحديد التوجه المستقبلي متضمناً المبادرات المطلوبة للإنتقال لبيئة العمل المستقبلية، وتوظيف موارد وقدرات المؤسسة والخدمات المقدمة والمستعان بها من قبل الغير بفعالية وإعتمادية عاليتين لتحقيق الاهداف الإستراتيجة للمؤسسة	التأكد من أن خدمات تقنية المعلومات والإتصالات المقدمة على مستوى من الجودة وتلبي إحتياجات المؤسسة الحالية والمستقبلية	07,14

مرفق رقم (3)

عمليات وأهداف الحوكمة والإدارة (Governance and Management Objectives)

رمز العملية	عنوان العملية	وصف العملية	هدف العملية	أرقام وأهداف المعلومات والتقنية المصاحبة لها ذات الصلة المباشرة
APO 10	إدارة المزودين Manage suppliers	إدارة خدمات تقنية المعلومات والإتصالات المقدمة من قبل الغير لدعم عمليات وأهداف المؤسسة، بما في ذلك آليات اختيار المزودين والأتصال بهم وإدارة التعاقدات معهم ومراقبة وتقييم أدائهم لفحص مدى الكفاءة والفعالية والإمتثال للشروط التعاقدية معهم	تقليل مستوى المخاطر قدر الإمكان نتيجة للإستعانة بالخدمات المُقدمة من قبل الغير والتأكد من الحصول على تلك الخدمات بأقل الأسعار الممكنة	04,07,09
APO 11	إدارة الجودة Manage quality	تعريف متطلبات الجودة في جميع عمليات المؤسسة وآلياتها وإجراءاتها، بما في ذلك الضوابط وعمليات المراقبة المستمرة واستخدام الممارسات والمعايير العالمية المعتمدة اللازمة للتطوير المستمر	تقديم حلول وخدمات تقنية تلبي إحتياجات العمل وتلقى رضا مستخدميها	05,07,13
APO 12	إدارة المخاطر Manage risk	الإستمرار بتحديد مخاطر تقنية المعلومات والإتصالات و تقييمها وضبطها ومراقبتها، للحفاظ عليها ضمن المستهدف من مستويات المخاطر المقبولة والمعتمدة في المؤسسة	تكامل إدارة تقنية المعلومات والإتصالات مع الإدارة الكلية للمخاطر في المؤسسة، والحفاظ على التوازن المطلوب بين المنافع والتكاليف	02,04,06,10,13
APO 13	إدارة أمن المعلومات Manage security	تعريف وتشغيل ومراقبة نظام إدارة أمن المعلومات	الحفاظ على حجم تأثير وأحتمالية حدوث متوقعة لحوادث تقنية المعلومات والإتصالات ضمن مستويات مقبولة لمدى تقبل المؤسسة على تحمل المخاطر	02,04,06,10,14

مرفق (3)

عمليات وأهداف الحوكمة والإدارة (Governance and Management Objectives)

رمز العملية	عنوان العملية	وصف العملية	هدف العملية	أرقام وأهداف المعلومات والتقنية المصاحبة لها ذات الصلة المباشرة
APO 05	إدارة محفظة المشاريع Manage Project Portfolio	تنفيذ مشاريع تقنية المعلومات والاتصالات المختلفة التي تلبي الأهداف والتوجه الاستراتيجي للمؤسسة، مع الأخذ بالحسبان محدودية المواد ومن ثم الاستغلال الأمثل لها، والعمل على تقديم وترتيب أولوية المشاريع وفقاً لمساهمتها في تحقيق الأهداف الاستراتيجية وعلى مستوى الفرص والمخاطر المقابلة لذلك، والعمل على توظيف منتجات المشاريع إلى آليات وأدوات تخدم عمليات المؤسسة، والاستمرار بمراقبة المنافع ومستوى القيمة المضافة لمحفظة المشاريع وإجراء التعديلات اللازمة في حِينهِ استناداً إلى التغذية الراجعة من عمليات المراقبة تلك، وعلى التغييرات في خطة عمل المؤسسة.	تعظيم الفائدة والاستغلال الأمثل للموارد من خلال إدارة شاملة جامعة لمحفظة مشاريع المؤسسة.	01،05،13
APO 06	إدارة الموازنة والتكلفة Manage Budget and Cost	إدارة الشؤون المالية لمواد تقنية المعلومات والاتصالات من خلال آليات عمل كل من الإدارة المالية وإدارة تقنية المعلومات والاتصالات في المؤسسة، بما في ذلك إعداد الموازنات ودراسة والتكاليف والمنافع وترتيب الأولويات من خلال استخدام أسس ومعايير موضوعية موحدة معتمدة في المؤسسة بهذا الشأن، والعمل بالتشاور معا ذوي المصلحة بتعديل المخصصات المرصودة وبما يخدم الأهداف الاستراتيجية والتكتيكية للمؤسسة.	توطيد العلاقة المشتركة بين إدارة تقنية المعلومات والاتصالات وذوي المصلحة في المؤسسة لضمان الاستغلال الأمثل لمواد التقنية وتقديم المعلومات بهذا الشأن بشفافية عالية تُسهّل عمليات المسائلة وتقدير حجم المنافع و القيمة المضافة، وتسهيل آليات اتخاذ القرار في توظيف موارد تقنية المعلومات والاتصالات.	05،06

مرفق (3)

عمليات وأهداف الحوكمة والإدارة (Governance and Management Objectives)

رمز العملية	عنوان العملية	وصف العملية	هدف العملية	أرقام وأهداف المعلومات والتقنية المصاحبة لها ذات الصلة المباشرة
APO 07	إدارة الموارد البشرية Manage Human Resources	توظيف منهجية تضمن إيجاد الهياكل التنظيمية وخطوط الاتصال المؤسسي الأفقي والعمودي، وتوظيف العنصر البشري الماهر والكفوء وتوزيع الصلاحيات والمهام والأدوار والمسؤوليات، وإيجاد خطط التدريب والتعلم المستمر، وتحفيز الموظفين بشكل دائم للحصول على الأداء المطلوب.	الاستغلال الأمثل للمواد البشرية لخدمة أهداف المؤسسة.	01،11،13،16،17
APO 08	إدارة العلاقات Manage Relationship	إدارة العلاقات بين إدارة تقنية المعلومات والاتصالات وباقي إدارات المؤسسة لضمان اتصال مؤسسي دائم وشفاف يدعم المصلحة المشتركة في تحقيق أهداف المؤسسة ضمن حدود الموازنات والمخاطر المقبولة والمعتمدة، ومد جسور الثقة من خلال لغة تفاهم مشتركة تعزز روح الإيجابية في المبادرة باتخاذ القرارات وتحمل المسؤوليات حيالها.	تحسين النتائج وزيادة مستوى الثقة والاعتماد الكفوء لمواد تقنية المعلومات والاتصالات.	01،07،12،17
APO 09	إدارة اتفاقيات الخدمات Manage Service Agreement	توافق مستوى جودة الخدمات المتعلقة بتقنية المعلومات والاتصالات مع توقعات واحتياجات المؤسسة بما في ذلك آليات تعريف وتحديد وتصميم وطلب تلك الخدمات وتوثيق التعاقدات مع الغير في شأنها، و وضع المعايير للمراقبة المستمرة لجودة ومستوى تلك الخدمات.	التأكد من أن خدمات تقنية المعلومات والاتصالات المقدمة على مستوى من الجودة وتُلَبِي احتياجات المؤسسة الحالية والمستقبلية.	07،14

مرفق (3)

عمليات وأهداف الحوكمة والإدارة (Governance and Management Objectives)

رمز العملية	عنوان العملية	وصف العملية	هدف العملية	أرقام وأهداف المعلومات والتقنية المصاحبة لها ذات الصلة المباشرة
APO 10	إدارة المزوِّدين Manage Suppliers	إدارة خدمات تقنية المعلومات والاتصالات المُقَدَمة من قبل الغير لدعم عمليات وأهداف المؤسسة، بما في ذلك آليات اختيار المزوّدين والاتصال بهم وإدارة التعاقدات معهم ومراقبة وتقييم أدائهم لفحص مدى الكفاءة والفاعلية والامتثال للشروط التعاقدية معهم.	تقليل مستوى المخاطر قدر الإمكان نتيجة للاستعانة بالخدمات المُقَدّمة من قبل الغير والتأكد من الحصول على تلك الخدمات بأقل الأسعار الممكنة.	04،07،09
APO 11	إدارة الجودة Manage Quality	تعريف متطلبات الجودة في جميع عمليات المؤسسة وآلياتها وإجراءاتها، بما في ذلك الضوابط وعمليات المراقبة المستمرة واستخدام الممارسات والعمل والمعايير العالمية المعتمدة اللازمة للتطوير المستمر.	تقديم حلول وخدمات تقنية تُلَبِي احتياجات العمل وتَلقَى رضا مستخدميها.	05،07،13
APO 12	إدارة المخاطر Manage Risk	الاستمرار بتحديد مخاطر تقنية المعلومات والاتصالات وتقييمها وضبطها ومراقبتها، للحفاظ عليها ضمن المستهدف من مستويات المخاطر المقبولة والمعتمدة في المؤسسة.	تكامل إدارة مخاطر تقنية المعلومات والاتصالات مع الإدارة الكلية للمخاطر في المؤسسة، والحفاظ على التوازن المطلوب بين المنافع والتكاليف.	02،04،06،10،13
APO 13	إدارة أمن المعلومات Manage Security	تعريف وتشغيل ومراقبة نظام إدارة أمن المعلومات.	الحفاظ على حجم تأثير واحتمالية حدوث متوقعة لحوادث تقنية المعلومات والاتصالات من مستويات مقبولة لمدى تقبل المؤسسة على تحمل المخاطر.	02،04،06،10،14

مرفق (3)

عمليات وأهداف الحوكمة والإدارة (Governance and Management Objectives)

رمز العملية	عنوان العملية	وصف العملية	هدف العملية	أرقام وأهداف المعلومات والتقنية المصاحبة لها ذات الصلة المباشرة
عمليات البناء (التطوير) والشراء والتشغيل (BAI) Build, Acquire and Implement				
BAI 01	إدارة البرامج والمشاريع Manage Programme and Project	إدارة جميع مشاريع المؤسسة لتحقيق الأهداف الإستراتيجية بشكل تعاوني بين إدارة تقنية المعلومات والاتصالات وباقي الإدارات المعنية، من خلال آليات التخطيط والضبط والتنفيذ للمشاريع والاستمرار بتقييم المشاريع في مراحل ما بعد التنفيذ.	ضمان تحقيق المنافع من إدارة المشاريع وتقليل مستوى المخاطر وتكاليف التأخير من خلال التواصل الصحيح بين المستخدمين وإدارة تقنية المعلومات والاتصالات.	01،04،05،13
BAI 02	إدارة تعريف المتطلبات والإحتياجات Manage Requirements Definition	تحليل الاحتياجات والمتطلبات من حلول تقنية المعلومات والاتصالات قبل الشروع بشراء وتطوير تلك الحلول بما يشمل آليات العمل والبرامج والبيانات/ المعلومات والبنية التحتية والخدمات، للتأكد من تماشيها والأهداف الاستراتيجية للمؤسسة، والتنسيق لدى دراسة الخيارات المطروحة مع مستخدمي التقنية، بما في ذلك دراسة الجدوى وتحليل المخاطر والتكاليف والمنافع والموافقات المطلوبة.	توفير حلول مجدية تُلَبِي احتياجات العمل بأقل المخاطر.	01،07،12

مرفق (3)

عمليات وأهداف الحوكمة والإدارة (Governance and Management Objectives)

رمز العملية	عنوان العملية	وصف العملية	هدف العملية	أرقام وأهداف المعلومات والتقنية المصاحبة لها ذات الصلة المباشرة
BAI 03	إدارة تحديد الحلول والبناء Manage Solutions Identification and Build	اختيار وتطوير حلول تقنية المعلومات والاتصالات تُلَبِي متطلبات العمل وإحتياجاته، تشمل آليات تصميم وتطوير وشراء والاستعانة بالغير. تشمل إدارة التعريفات (Configuration and Management) وآليات فحص الحلول، وإدارة الاحتياجات وتحديدها، وعمليات الصيانة والتطوير المستمر للبرمجيات وآليات العمل والبيانات / المعلومات والبنية التحتية والخدمات.	توفير حلول تقنية المعلومات والاتصالات بالوقت المطلوب وبأقل التكاليف لخدمة أهداف المؤسسة.	07
BAI 04	إدارة التوافرية والطاقة الإستعابية Manage Availability and Capacity	عمل التوازن المطلوب بتوفير خدمات تقنية المعلومات والاتصالات بين الحاضر والمستقبل مع الأخذ بالحسبان التكاليف ومستوى الأداء، بما في ذلك تحديد القدرات الحالية والمستقبلية استناداً إلى احتياجات وخطط المؤسسة، من خلال تحليل الأثر في الأعمال وتقييم المخاطر.	توافرية خدمات تقنية المعلومات والاتصالات الإدارة الفعالة للموارد وتحسين أداء الأنظمة من خلال توقع الطاقة الاستيعابية المستقبلية.	07،11،14
BAI 05	إدارة تمكين التغيير المؤسسي Manage Organizational Change and Enablement	تحسين احتمالية نجاح عمليات التغيير المؤسسي بسرعة وبأقل المخاطر بما يشمل آليات التغيير وعمليات المؤسسات وتقنية المعلومات والاتصالات والأفراد.	إعداد وضمان إلتزام الأفراد بالتغيير المؤسسي بنجاح وبأقل المخاطر.	08،13،17

مرفق (3)

عمليات وأهداف الحوكمة والإدارة (Governance and Management Objectives)

رمز العملية	عنوان العملية	وصف العملية	هدف العملية	أرقام وأهداف المعلومات والتقنية المصاحبة لها ذات الصلة المباشرة
BAI 06	إدارة التغييرات Manage Change	إدارة التغييرات كافّة من خلال توفير الضوابط اللازمة من مبادئ وسياسات التغيير تشمل التغييرات الطارئة والمستعجلة والتغيير على عمليات المؤسسة والبرمجيات والبنية التحتية للتقنية، فضلاً عن توفير معايير وإجراءات للتغيير تتضمن قياس التغيير في العمليات، والأولويات في التغيير، والموافقات المطلوبة للتغيير وإجراءات التغييرات الطارئة، واستخراج تقارير التَتَبُع للتغيرات، الإغلاق والتوثيق.	إجراء التغييرات المطلوبة بالسرعة الممكنة وبأقل المخاطر المحتملة لأي آثار سلبية في مصداقية التغييرات.	04،07،10
BAI 07	إدارة قبول التغيير والإنتقال Manage Change Acceptance and Transitioning	تشغيل حلول تقنية المعلومات والاتصالات بعد أخذ موافقات القبول الرسمية من إدارة المستخدمين، بما يشمل عمليات التخطيط قبل الشروع بالتنفيذ، وترحيل البيانات، وقبول نجاح فحوصات الاستخدام.	تشغيل حلول التقنية بأمان وبما يتوافق والتوقعات.	08،12
BAI 08	إدارة المعرفة Manage Knowledge	توفير منظومات معارف محدّثة ومعتمدة عليها والمحافظة عليها، لدعم عمليات المؤسسة والمساعدة في اتخاذ قرارات سليمة. إدارة دورة حياة المعارف (التخطيط وجمع المعارف وتبويبها وتنظيمها وتحديثها واستخدامها وحذفها)	تقديم المعارف للموظفين لتمكّنهم من أداء واجباتهم منافع مستويات مستوى الإنتاجية.	09،17

مرفق (3)

عمليات وأهداف الحوكمة والإدارة (Governance and Management Objectives)

رمز العملية	عنوان العملية	وصف العملية	هدف العملية	أرقام وأهداف المعلومات والتقنية المصاحبة لها ذات الصلة المباشرة
BAI 09	إدارة الأصول Mange Assets	إدارة أصول تقنية المعلومات والإتصالات على مدار دورة حياتها للتأكد من تحقيقها المنافع المرجوة بأقل التكاليف الممكننة، وبأنها تتناسب والعمليات المشغلة ضمنها، وبأنها معدودة ومحمية، وأنّ الأصول المهمة لدعم العمليات المصرفية الحسّاسة متوافرة بشكل مستمر ومعتمد عليها، وإدارة تراخيص البرمجيات للتأكد من كفايتها لدعم عمليات المؤسسة وبأن إستخدامها هو ضمن حدود القوانين المعتمدة.	إدارة أصول تقنية المعلومات والإتصالات والإستخدام الأمثل لها.	06،11
BAI 10	إدترة التكوين Manage Configuration	وصف كل من الموارد الرئيسية للمؤسسة من جهة وقدرات تقنية المعلومات والإتصالات المطلوبة لتقديم خدمات التقنية من جهة أُخرى وتعريف العلاقة بينهما، بما يشمل جمع المعلومات المختلفة ووضع الأسس المعيارية، وإخضاعها لعمليات المراجعة الدورية والتدقيق المستمر.	توفير معلومات كافية عن خدمات وخصائص أصول تقنية المعلومات والاتصالات لإدارة تلك الأصول بكفاءة، ومعرفة أثر تغيير تلك الخصائص في العمل من ناحية أمن المعلومات والتقنية.	02،11،14
عمليات توصيل الخدمة والدعم Delivery, Service and Support (DSS)				
DSS 01	إدارة العمليات Mange Operations	تنسيق وتنفيذ النشاطات وعمليات تقنية المعلومات والاتصالات الداخلية المعتمد فيها على الغير بما في ذلك وضع معايير وسياسات التشغيل والمراقبة.	تشغيل عمليات تقنية المعلومات والاتصالات بحسب الخطط الموضوعة بهذا الصدد.	04،07،11

مرفق (3)

عمليات وأهداف الحوكمة والإدارة (Governance and Management Objectives)

رمز العملية	عنوان العملية	وصف العملية	هدف العملية	أرقام وأهداف المعلومات والتقنية المصاحبة لها ذات الصلة المباشرة
DSS 02	إدارة طلبات الخدمة والحوادث Manage Service Request and Incidents	الاستجابة في الوقت المحدد لطلبات المستخدمين ولكل أنواع حوادث تقنية المعلومات والاتصالات، إعادة تشغيل عمليات التقنية بعد الانقطاع، وتوثيق طلبات المستخدمين، وإجراء التحقيقات اللازمة لاختراقات التقنية وتشخيصها وإعلام الإدارات المعنية بشأنها ومعالجتها.	رفع مستوى الإنتاجية وتقليل معدل الانقطاعات من خلال الاستجابة السريعة لمتطلبات المستخدمين ومعالجة حوادث تقنية المعلومات والاتصالات.	04،07
DSS 03	إدارة المشاكل Manage Problems	تحديد وتصنيف أعطال تقنية المعلومات والاتصالات بما في ذلك مسبباتها الرئيسية للوقاية من الحوادث، وتقديم التوصيات والتحسينات المطلوبة.	زيادة معدل التوافرية ومستوى خدمات تقنية المعلومات والاتصالات وخفض التكاليف وتحسين مستوى الرضا من قبل مستخدمي التقنية من خلال خفض عدد الأعطال.	04،07،11،14
DSS 04	إدارة الإستمرارية Manage Continuity	إنشاء خطة لإدارة استمرارية عمليات المؤسسة وتقنية المعلومات والاتصالات وتطويرها، لضمان استمرارية عمليات المؤسسة الحسّاسة والحرجة لمواجهة أسباب الانقطاع وحوادثه ضمن الحدود المستهدفة بهذا الشأن.	ضمان استمرارية تشغيل عمليات المؤسسة الحرجة وعمليات تقنية المعلومات والاتصالات الداعمة لها لمواجهة حوادث الانقطاع ضمن الحدود المستهدفة.	04،07،14
DSS 05	إدارة خدمة أمن المعلومات Manage Security Services	حماية معلومات المؤسسة والإبقاء عليها بمستوى مخاطر مقبول ضمن إطار سياسات أمن المعلومات وحمايتها للمؤسسة، وإنشاء والاستمرار بتحديث مهام معلومة مسؤوليات إدارة أمن المعلومات، والامتيازات للنفاذ والاستخدام ومراقبة الاستخدام لمواد التقنية.	تقليل الأثر السلبي في عمليات المؤسسة جرّاء الحوادث ونقاط الضعف لأمن المعلومات.	02،04،10

مرفق (3)

عمليات وأهداف الحوكمة والإدارة (Governance and Management Objectives)

رمز العملية	عنوان العملية	وصف العملية	هدف العملية	أرقام وأهداف المعلومات والتقنية المصاحبة لها ذات الصلة المباشرة
DSS 06	إدارة ضوابط عمليات المؤسسة Manage Business Process Control	تعريف ضوابط العمليات للمؤسسة، وتحديدها والإستمرار في توظيفها، الكفيلة بتحقيق المتطلبات الأمنية المحددة للمعلومات والتقنية المصاحبة لها، تلك العمليات سواء المُنَفَذَة داخلياً أو المعتمد فيها على الغير.	الحفاظ على سلامة ومصداقية وأمن المعلومات المعالجة من قبل عمليات المؤسسة أو عمليات الغير المستعان بها.	04،07
عمليات الرقابة والتقييم والقياس Monitor, Evaluation and Assess (MEA)				
MEA 01	مراقبة وتقييم وتقدير الأداء والمطابقة Monitor, Evaluation and Assess Performance and Conformance	جمع والتحقق وتقييم أهداف ومعايير قياس أداء عمليات المؤسسة بما فيها عمليات تقنية المعلومات والاتصالات وإجراءات العمل، ومراقبة تلك العمليات للتأكد من تحقيق المستهدفات بشأنها ورفع التقارير اللازمة بهذا الشأن دورياً.	الشفافية بشأن مستوى الأداء تجاه تحقيق الأهداف.	04،07،11،15
MEA 02	مراقبة نظام الضبط والرقابة الداخلية للمؤسسة وتقييمه و تقديره Monitor, Evaluate and Assess the System of Internal Control	المراقبة المستمرة والتقييم لبيئة الضوابط الداخلية بواسطة كل من التقييم الذاتي والتقييم المستقل، وتمكين الإدارة من تحديد الاختلالات في الضوابط المفعّلة لإتخاذ التحسينات والتصحيحات المطلوبة، التخطيط والتنظيم والتحديث لمبادئ وقواعد التقييم لنظام الضبط والرقابة الداخلي للمؤسسة.	تقييم المعلومات بشفافية لذوي المصلحة بشأن مدى سلامة وملائمة نظام الضبط والرقابة الداخلية لعمليات المؤسسة، في المساهمة بتحقيق أهداف المؤسسة من خلال الفهم الصحيح لمستويات المخاطر المتبقية في المؤسسة (Residual Risk)	02،04،15

مرفق (3)

عمليات وأهداف الحوكمة والإدارة (Governance and Management Objectives)

رمز العملية	عنوان العملية	وصف العملية	هدف العملية	أرقام وأهداف المعلومات والتقنية المصاحبة لها ذات الصلة المباشرة
MEA 03	مراقبة وتقييم وتقدير مستوى الامتثال للقوانين والأنظمة والضوابط الخارجية Monitor, Evaluate and Assess Compliance with External Requirements	تقييم مستوى الامتثال للممارسات لكل من عمليات المؤسسة المرتكزة على عمليات تقنية المعلومات والاتصالات للقوانين والأنظمة والضوابط المعتمدة ولشروط التعاقد مع الغير، والحصول على تأكيدات بتحديد المتطلبات القانونية والتعاقدية ومستوى الامتثال لها، وعّدّ مواضيع الامتثال لمتطلبات التقنية.	التأكد من إمتثال المؤسسة للقوانين والأنظمة والضوابط.	02,04

المرفق رقم (4) : نموذج تقرير تدقيق المعلومات والتقنية المصاحبة لها

(إسم المُدقَّق أو مؤسسة التدقيق)

تقرير تقييم (مخاطر – ضوابط) المعلومات **والتقنية المصاحبة لها للمؤسسة / لمصرف .....** **الإدارة العامة (الفرع)**
مدة التدقيق **من تاريخ – إلى تاريخ** **عدد أيام العمل** **( ) يوماً**

إسم المُدقِّق المسؤول	مع إرفاق ملحق على المؤهلات والخبرات وصُوَر عن الشهادات الأمنية والزمالات السارية
أسماء أعضاء فريق التدقيق	مع إرفاق ملحق على المؤهلات والخبرات وصُوَر عن الشهادات الأمنية والزمالات السارية

المرفق رقم (4) : نموذج تقرير تدقيق المعلومات والتقنية المصاحبة لها

أولاً: نموذج إطلاع وتوصيات المجلس على التقرير:

ثانياً: المُقَدّمة: (لاعتبارات فنية من المسموح استخدام اللغة الإنجليزية في كتابة التقرير)

1. **نتائج التقييم الكلي (Composite Risk Rating): تقييم (مخاطر – ضوابط): تقييم المعلومات والتقنية المصاحبة لها :-**

تمّ تقييم (مخاطر – ضوابط) المعلومات والتقنية المصاحبة لها لدى المؤسسة بدرجة ( ) استناداً إلى **محاور التقييم الآتية**، علماً بأن درجات التقييم تُقَسّم تنازلياً على خمس مستويات (عبارة عن سُلّم التقييم الكلي للمخاطر): 1- قوي 2- مرضي 3- عادل 4- حدي 5- غير مرضي:

أ- حوكمة وإدارة المعلومات والتقنية المصاحبة لها، وثم تقييمها بدرجة ( ).

ب- البرامج التطبيقية، وثم تقييمها بدرجة ( ).

ت- إدارة البيانات.

ث- أجهزة الكمبيوتر الرئيسية وإدارتها، وثم تقييمها بدرجة ( ).

ج- الشبكات، وثم تقييمها بدرجة ( ).

ح- خطط الطوارئ واستمرارية العمل، والحماية المادية والبيئية، وثم تقييمها بدرجة ( ).

2. **منهجية الفحص والتقييم:**

تمّ اتّباع منهجية التقييم الآتية بشأن نقاط الضعف الواردة في المحاور المذكورة أعلاه:

أ. **كمية المخاطر:**

تم احتسابها وتقديرها على أساس المعادلة الآتية:

المخاطر الحالية = (نقطة الضعف x التهديد) (الملحوظة) x الأهمية – الظو ابط المفعلة

أي: إنَ تقدير كمية المخاطر الحالية (Current Risk) تمّ بناءَ على أهمية نقطة الضعف والتهديد الذي تُشَكِلَهُ (الملحوظة) مع الأخذ بالحسبان المخففات المتمثلة بالضوابط المفعّلة. إذ تمّ تقسيم درجات كمية المخاطر تنازلياً على ثلاث مستويات: (عالي، متوسط، منخفض) (من الممكن اختيار سُلّم تقييم أكثر تفصيلاً)، وتمّ تقسيم الأهمية (المقصود بها المخاطر الموروثة Inherent Risk) تنازلياً على أربعة مستويات (حرج، جوهري، متوسط، قليل)، وتمَ تقسيم قوة الضوابط تنازلياً على أربعة مستويات (ممتاز، جيد، ملائم، ضعيف). علما بأنه تمّ اتباع **أسلوب التدقيق المبني على المخاطر** من حيث الاهتمام بتقييم الجوانب ذات المخاطر والأثر السلبي الأعلى في عمليات المؤسسة.

ب. نوعية إدارة المخاطر (Quality of Risk Management):

تمّ تقديرها إستناداً إلى نوعية إدارة المؤسسة لمخاطر التشغيل من حيث توافر استراتيجية أو سياسة مخاطر مُقرَّة من المجلس تُجَسِّد رؤية المصرف، ومقدار الرغبة في تحمل المخاطر (Risk Appetite)، فضلاً عن الاستناد إلى وجود هيكل إداري مؤسسي لتطبيق الاستراتيجية المذكورة وآليات تحديد وتعريف وقياس وضبط ومراقبةالمخاطر، مع الأخذ بالحسبان درجة الاستجابة والتعاون ومدى وجود خطط مستقبلية للتصحيح ونوعية إدارة المخاطر من حيث تقليل المخاطر (Mitigate)، أو نقل المخاطر (Transfer)، أو قبول المخاطر (Accept)، أو تجنب المخاطر (Avoid)، أو رفض المخاطر (Reject)، وقد تمّ تقسيم نوعية إدارة المخاطر تنازلياً على ثلاثة مستويات (قوي، مقبول، ضعيف) (من الممكن اختيار سُلَّم تقييم أكثر تفصيلاً).

المرفق رقم (4): نموذج تقرير تدقيق المعلومات والتقنية المصاحبة لها

(اسم المُدقق أو مؤسسة التدقيق)

تقرير تقييم مخاطر- ضوابط المعلومات والتقنية المصاحبة لها للمؤسسة المصرف..... **الإدارة العامة (الفرع)**
مدة التدقيق **من تاريخ - إلى تاريخ عدد أيام العمل ( ) يوماً**

اسم المدقق المسؤول	**مع إرفاق ملحق عن المؤهلات والخبرات وصور عن الشهادات المهنية**
أسماء أعضاء فريق التدقيق	**مع إرفاق ملحق عن المؤهلات والخبرات وصور عن الشهادات المهنية**

المرفق رقم (4): نموذج تقرير تدقيق المعلومات والتقنية المصاحبة لها

أولاً: نموذج إطلاع وتوصيات المجلس على التقرير:

ثانياً: المقدمة: الاعتبارات فنية من المسموح استخدام اللغة الإنجليزية في كتابة التقرير)

1 نتائج التقييم الكلي (Composite Risk Rating) تقييم مخاطر - ضوابط تقييم المعلومات والتقنية المصاحبة لها:

تم تقييم (مخاطر - ضوابط) المعلومات والتقنية المصاحبة لها لدى المؤسسة بدرجة ( ) استنادا إلى محاور التقييم الآتية، علما بأن درجات التقييم تقسم تنازليا على خمس مستويات عبارة عن مسلم التقييم الكلى للمخاطر) 1 قوي -2 مرضي - عادل 4- حدى 5- غير مرضى.

أ حوكمة وإدارة المعلومات والتقنية المصاحبة لها، وتم تقييمها بدرجة ( ).

ب البرامج التطبيقية، وتم تقييمها بدرجة ( ).

ت إدارة البيانات.

ت أجهزة الكمبيوتر الرئيسة وإدارتها، وتم تقييمها بدرجة ( ).

ج الشبكات، وتم تقييمها بدرجة ( ).

ح خطط الطوارئ واستمرارية العمل، والحماية المادية والبيئية، وتم تقييمها بدرجة ( ).

2 منهجية الفحص والتقييم : تم اتباع منهجية التقييم الأتية بشأن نقطة الضعف الواردة في المحاور المذكورة في أعلاه:

كمية المخاطر.

تم احتسابها وتقديرها على أساس المعادلة الآتية :

المخاطر الحالية = (نقطة الضعف x التهديد) (الملحوظة) × الأهمية - الضوابط المفعلة.

أي: إن تقدير كمية المخاطر الحالية (Current Risk) تم بناءً على أهمية نقطة الضعف والتهديد الذي تشكله (الملحوظة) مع الأخذ بالحسبان المخففات المتمثلة بالضوابط المفعلة إذ تم تقسيم درجات كمية المخاطر تنازليا على ثلاثة مستويات عالي متوسط منخفض) (من الممكن اختبار مسلم تقديم أكثر تفصيلا)، وتم تقسيم الأهمية المقصود بها المخاطر الموروثة Inherent Risk) تنازليا على أربعة مستويات (حرج، جوهري، متوسط قليل)، وتم تقسيم قوة الضوابط تنازليا على أربعة مستويات (ممتاز، جيد، ملائم، ضعيف) علما بأنه تم اتباع أسلوب التدقيق المبني على المخاطر من حيث الاهتمام بتقييم الجوانب ذات المخاطر والأثر السلبي الأعلى في عمليات المؤسسة.

ب نوعية إدارة المخاطر (Quality of Risk Management) تم تقديرها استنادا إلى نوعية إدارة المؤسسة لمخاطر التشغيل من حيث توافر استراتيجية أو سياسة مخاطر فقرة من المجلس تجسد رؤية المصرف، ومقدار الرغبة في تحمل المخاطر (Risk Appetite) فضلاً عن الاستناد إلى وجود هيكل إداري مؤسسي لتطبيق الاستراتيجية المذكورة وآليات تحديد وتعريف وقياس وضبط ومراقبة المخاطر، مع الأخذ بالحسبان درجة الاستجابة والتعاون ومدى وجود خطط مستقبلية للتصحيح ونوعية إدارة المخاطر من حيث تقليل المخاطر (Mitigate)، أو نقل المخاطر (Transfer)، أو قبول المخاطر (Accept)، أو تحلب المخاطر (Avoid)، أو رفض المخاطر (Reject). وقد تم تقسيم نوعية إدارة المخاطر تنازليا على ثلاثة مستويات قوي، مقبول ضعيف) (من الممكن اختيار مسلم تقييم أكثر تفصيلاً.

المرفق رقم (4) نموذج تقرير تدقيق المعلومات والتقنية المصاحبة لها

وقيما ياتي جدول يلخص تقييم المنحوانات الواردة في متن التقرير، ويحدد المسؤولية:

رمز الملحوظة	الملحوظة	المسؤولية	كمية المخاطر	نوعية وإدارة المخاطر
رقم تسلسل المحور: التسلسل في المحورنفسه	عنوان الملحوظة	رتبة الشخص أو الجهة/ الجهات المسؤولة	مع اختيار لون درجة المخاطر	مع اختيار لون درجة المخاطر

3. مناقشة التقرير: تم بتاريخ إرسال التقرير إلى إدارة المؤسسة تمهيدا لعقد اجتماع مع الأطراف المعنية لمناقشة محتوياته، هذا وقد تم بتاريخ / الاجتماع مع إدارة المؤسسة نملة مكل، وقد حقق الاجتماع أهدافه من حيث:

أ. التاكد من مصداقية محتويات تقرير الدقيق.

ب. التاكد من الفهم الصحيح المحتويات تقرير التدقيق من قبل إدارة المؤسسة.

الاتفاق على التواريخ الواجب على ادارة المؤسسة الالتزام بها لتصحيح الثغرات ونقاط الضعف الواردة في تقرير التدقيق.

4. محددات التدقيق

يتم ذكر اية محددات أثرت سلنا في مجريات أو نتائج مهمة التدقيق بما في ذلك على سبيل المثال لا الحصر عدم التزود بالبيانات والمعلومات المطلوبة بالشكل الصحيح وبالموعد المطلوب ومدى تعاون إدارة المؤسسة مع المدقق وتسهيل مهمته، وأية معيقات أو محددات أخرى

5مؤهلات وخبرات المحقق المسؤول وأعضاء فريق التحقيق

(يتم ذكرها)

ثالثا: متن :التقرير ونعرض فيما باتي تفاصيل التقييم في أعلاه:

(وفيها محاور تقييم ستة يجب أن تغطي بالحد الأدنى متطلبات ضوابط حوكمة وإدارة المعلومات والتقنية المصاحبة لها)

1حوكمة وإدارة المعلومات والتقنية المصاحبة لها.IT Governance & Mgt

تم تقيمها بدرجة - يتم استخدام سلم تقييم المخاطر Component Risk Rating المذكور في أعلاه Composite Risk Rating) وذلك على النحو الاتي:

الملحوظة (1:1) حوكمة المعلومات والتقنية المصاحبة لها (ذكرت على سبيل المثال ويتم توصيف باقي الملحوظات في المحور)

تقييم الملحوظة (1:1)								
مدى الاهمية	حرج	×	جوهري		متوسط		قليل	
تقييم الضوابط	ممتاز		جيد		ملائم		ضعيف	×
كمية المخاطر	عالي	×	متوسط		منخفض			
نوعية وادارة المخاطر	قوي		مقبول		ضعيف	×		

مرفق رقم (4) نموذج تقرير تدقيق المعلومات والتقنية المصاحبة لها

يتم توصيف الثغرات (Vulnerabilities) التي تشكل نقط ضعف في الضوابط والأنظمة والإجراءات، فضلا عن توصيف التهديدات (Threats) التي يمكن التعرض لها، وبالمحصلة بتم توصيف الأثر (Impact) سواء الأثر المالي أو التشغيلي أو القانوني أو أثر السمعة ... الخ.

التوصية:

يتم توصيف الإجراءات المطلوب اتخاذها من قبل إدارة المؤسسة للوصول بالمخاطر إلى الحد المقبول.

رد إدارة المؤسسة:

يتم ذكر رد إدارة المؤسسة

2. البرامج التطبيقية (Applications):

تم تقييمها بدرجة)، وذلك على النحو الآتي:

3 إدارة البيانات :(Data Management) تم تقييمها بدرجة ()، وذلك على النحو الآتي

4 أجهزة الكمبيوتر الرئيسة بما فيها انظمة التشغيل والبرمجيات الأخرى: (Servers)

تم تقييمها بدرجة ()، وذلك على النحو الآتي:

5 شبكات الكمبيوتر المحلية والواسعة والانترنت والإنترانت والأنظمة المساندة :Networks) تم تقديمها بدرجة ()، وذلك على النحو الآتي:

6 خطط الطوارئ وخطط استمرارية العمل والحماية المادية والبيئيةBusiness Continuity and disaster recovery

plans, physical and environmental securityتم تقديمها بدرجة ()، وذلك على النحو الآتي:

رابعا جدول بالملحوظات العالقة ولم تعالج من سنوات سابقة:

الملحوظات	وصف الملحوظة	كمية المخاطر	نوعية إدارة المخاطر	الإجراء المتخذ من قبل إدارة المؤسسة وتاريخه	التوصية

مرفق (5) محاور تدقيق المعلومات والتقنية المصاحبة له

حوكمة تكنولوجيا المعلومات والاتصالات IT Governance
مدى كفاية وكفاءة تحقيق عمليات حوكمة تكنولوجيا المعلومات والاتصالات الواردة في المرفق رقم (٣)، وضوابط مصرف ليبيا المركزي المتعلقة بهذا الشأن من خلال تطبيق عمليات الرقابة والتقييم والقياس (MEA) الواردة في المرفق المذكور ألفا
مستوى التوافق الاستراتيجي بين أهداف تكنولوجيا المعلومات والاتصالات
مدى مستوى رضا المستخدمين على إدارة تقنية المعلومات والخدمات والمنتجات والدعم الفني المقدم
كفاية وفعالية السياسات الخاصة بأمن المعلومات وحمايتها
مدى كفاية لجان تقنية المعلومات من حيث المهام ونطاق العمل والنشاط
مدى كفاية الهياكل التنظيمية وضمان عدم تضارب المصالح وفصل المهام المتعارضة بطبيعتها
مدى كفاية وكفاءة ومهارات ومؤهلات المعنيين بالتدقيق الداخلي والتدقيق الخارجي والمستشارين في مجال تقنية المعلومات
مدى كفاية وشمولية الوصف الوظيفي لكوادر تقنية المعلومات والاتصالات والتدقيق الداخلي لتقنية المعلومات والاتصالات ولأمن المعلومات
مدى كفاية إدارة مخاطر تقنية المعلومات والاتصالات والمخاطر التشغيلية، والممارسات العملية في آليات اتخاذ القرار المبني على المخاطر بما فيها مخاطر تقنية المعلومات والمخاطر الاستراتيجية
مدى كفاية وتنظيم إدارة أمن المعلومات من حيث الهياكل التنظيمية وتوظيف الموارد المختلفة بما في ذلك العنصر البشري
مدى توافر وكفاية وتنظيم إدارة محفظة المشاريعProject Portfolio Management
مدى امتثال مجلس الإدارة والإدارة التنفيذية لضوابط حوكمة تقدية المعلومات والاتصالات
مدى استخدام أدوات وبرامج لكشف الاحتبال (CAATS) مثل (ACL, IDEA) من قبل التدقيق
مدى وجود سياسات الاستعانة بالغير وكتابتها (التعهيد أو الاستاد)(Outsourcing)
مدى كفاية التوثيق للتعاقدات الخارجية والداخلية وملاحقها من حيث نتفصيل الخدمات المقدمة والمسؤوليات حيالها
مدى كفاية البرامج التدريبية وتنظيمها لزيادة ونشر مستوى الوعي بالممارسات السليمة لأمن المعلومات وحمايتها، لكل من موظفي المؤسسة وزبائنه ومدى توافر معايير بهذا الشأن على شكل قواعد السلوك المهني

البرامج التطبيقية وإدارتها
مدى كفاية الإجراءات المعتمدة والمطبقة وكفاءتها، التي لعلى باليات تطوير وشراء وفحص وتشغيل البرامج
مدى كفاية وسلامة الإجراءات الخاصة بتعريف امتيازات الموظفين على البرامج المستخدمة بحسب طبيعة العمل (Role based access privileges)
مدى انخراط إدارة أمن المعلومات بمنح صلاحيات النفاذ والاستخدام للبرامج الحمناسة، والموافقة المسبقة عليها
فحص ضوابط إدخال البيانات على البرامج المناسة مثل وجودMaker.checker)
فحص مضوابط المخرجات والحفظ الأمن للوثائق الحساسة المستخرجة من البرامج المختلفة
فحص مدى سلامة البرامج في عمليات المعالجة Data Processing ومدى مصداقية المدخلات والمخرجات
فحص ضوابط تشغيل القنوات الإلكترونية ونظم الدفع الالكتروني
مدى استخدام برامج Computer Aided System Engineering في عمليات التوثيق والمتابعة
مدى حصول البرامج الرئيسة على شهادات تأهيل من مؤسسات تصنيف دولية معروفة(Accreditation)
مدى الامتثال لضوابط مصرف ليبيا المركزي بشأن التصنيف الأني للتسهيلات

إدارة قواعد البيانات
مدى كفاءة وتفعيل سياسات الإزاحة للبيانات، وإدارة قواعد البيانات
مدى كفاءة وكفاية موظفين متخصصين في إدارة قواعد البيانات
مدى كفاءة وكفاية إجراءات مطبقة لمراقبة وتحسين الأداء لقواعد البيانات والبيانات بشكل عام
فحص ضوابط الحماية بشأن فصل صلاحيات إدارة قواعد البيانات عن البيانات نفسها للحماية من مخاطر الاختراق والتعديل غير المصرح به من قبل ضابط قواعد البيانات
مدى كفاءة وتفعيل إجراءات النسخ الاحتياطي
مدى كفاءة وتفعيل عمليات مراقبة الاستخدامDBA) من قبل إدارة منفصلة مثل أمن المعلومات
مدى كفاءة وتفعيل والاستناد إلى اليات مثل Error Dictionary لمعالجة أخطاء ومشاكل إدارة البيانات

إدارة أجهزة الكمبيوتر الرئيسة
مدى كفاءة وتفعيل إجراءات النسخ الاحتياطي لتكوينات الأنظمة (Systems Configurations)
مدى كفاءة وتفعيل إجراءات مراقبة أداء الأجهزة
مدى كفاءة وتفعيل إجراءات فحص الأنظمة لدى كل تغيير (ترقية تطوير)
مدى كفاءة وتفعيل إجراءات مراجعة تقارير متابعة الاستخدام لمديري الأنظمة(Administrators Dogs ، وهل تراجع من قبل جهة منفصلة مثل Security Administrator)
مدى كفاءة وتفعيل إجراءات موثقة لمعالجة أخطاء التشغيل
مدى كفاءة وتفعيل إجراءات تغيير كلمات السر لنفاذ مديري الأنظمة (Administrators) والمستخدمين ذوي الامتيازات العليا
مدى كفاءة إجراءات فحوصات الاختراق وتحديد الثغرات وكفايتها (vilnerability assessment and penetration test)
فحص مستوى التوافرية لأجهزة الكمبيوتر الرئيسة
مدى كفاية عمليات فصل بيئة التطوير والفحص عن بيئة التشغيل

إدارة الشبكات(Networks)
مدى وجود سياسات تعريف وإدارة الشبكات وكفاءتها وتفعيلها
مدى استخدام الشبكات لنشر الوعي بممارسات أمن المعلومات وحمايتها، لموظفي وزبائن المؤسسة، وزيادته
مدى وجود مكتب المساعدة Help Desk وكفاءته
مدى كفاية موظفين مختصين في إدارة الشبكات Network Administrators وكفاءتهم
مدى كفاية إجراءات إدارة التغيير Change Management وكفاءتها
مدى الالتزام بالتراخيص للبرمجيات وحقوق الملكية الفكرية
مدى كفاية إجراءات مراقبة أداء الشبكات والأدوات المستخدمة في المراقبة، وفعاليتها
فحص مستوى التوافرية لعناصر الشبكات ومدى ملاءمتها لخطط استمرارية العمل
مدى كفاية إجراءات مراقبة الاستخدام للشبكات، وفعاليتها (مراقبة إشرافية من قبل مدير الشبكات أو من يفوضه، ومراقبة مستقلة من قبل إدارة أمن المعلومات)

قوة التشفير المستخدم لدى تراسل البيانات عبر الشبكات ذات النطاق الواسع WAN وتلك المفتوحة مع الغير
فحص مواصفات الجدران النارية Firewalls وتحديد المستوى من الOSI / ISO التي تعمل عليه (مثال على المستوى الثالث Network Layer أو المستوى السابع Application Layer) ومدى كفاية معايير الأمن والحماية السرية وخصوصية البيانات ومصداقيتها بصورة خاصة
مدى كفاية إجراءات إدارة منفصلة وفعاليتها، مثل أمن المعلومات بمراجعة التعديلات الحاصلة على(Firewall security policy CL) ومراقبتها، وعلى تتبع الاستخدام من قبل مدير الشبكة(Administrator)
مدى استخدام أجهزة IDS / IPS على الشبكات ومدى كفاية الإجراءات حيال عمليات المراجعة بشأنها، وفعاليتها
مدى كفاية ضوابط الحماية المفعلة لعمليات النفاذ عن بعد(Remote Access and Use)

إدارة خطط استمرارية العمل والأمن المادي والبيئي
مدى كفاية خطط استمرارية العمل وكفاءتها، بما في ذلك من توافرية لموارد تقنية المعلومات والاتصالات والعنصر البشري وإجراءات وتنظيم الخطط ضمن إطار الامتثال لضوابط مصرف ليبيا المركزي بهذا الشأن
مدى كفاية إجراءات جرد الأصول من أجهزة وبرامج ونظم المعلومات وفعاليتها
مدى كفاية الإجراءات الخاصة وفعاليتهابحماية الأجهزة المختلفة من النفاذ غير المصرح به، ومن الفيروسات، مثل النفاذ عبر الشبكات من خلال أجهزة كمبيوتر مجهزة بمنافذ(CD Rom, USB...etc)
مدى كفاية الإجراءات الخاصة بالحماية المادية لعناصر ومكونات الشبكات من النفاذ غير المصرح به مثل وجود (Open Ports) لعناصر الشبكات غير الفاعلة
مدى كفاية الإجراءات الخاصة بالحماية المادية لعناصر الشبكات(Switches, Router ...etc) من الوصول غير المصرح به
فحص متطلبات الأمن المادي والبيني لغرف تشغيل مراكز البيانات والاتصالات الرئيسة والبديلة، بناء على معايير تقييم مثل مدى ملاءمة الموقع، ودرجة حرارة ورطوبة مناسبة، وأرضية مرفوعة، ومكان وجود الغرفة في البداية، ووجود أجهزة إطفاء حريق الي ونوعها نوع الغاز المستخدم إذا كان مسموح باستخدامه بموجب المواصفة والعالمية)، وأجهزة إنذار وكشف الحريق وتسريب المياهوكاميرات المراقبة والتسجيلوسجل دخول الزوار، وحصر الدخول فقط للأشخاص المصرح لهم، والضوابط المستخدمة في ذلك
مدى كفاية إجراءات المُراجعة الدورية لملف زوار المؤسسة، ولغرفة تشغيل مراكز البيانات والإتصالات.

مرفق (6) منظومة السياسات (الحد الأدنى)

اسم السياسة	الغرض	النطاق
حوكمة تنظيم تكنولوجيا المعلومات والاتصالات	وضع القواعد والمعايير اللازمة لإدارة موارد تقنية المعلومات والاتصالات، بما في ذلك الشكل الإداري عمليات وخدمات مركزي أو لامركزي، والهياكل التنظيمية بما في ذلك النشاطات والمهام والمسؤوليات لإدارة تلك الموارد المعلومات والا بما في ذلك الموارد المالية.	عمليات وخدمات ومشاريع تقنية
امن المعلومات وحمايتها	وضع القواعد والمعايير اللازمة لضمان متطلبات الحماية ، والسرية والمصداقية والتوافرية، والامتثال جميع المعلومات لإدارة موارد تقنية المعلومات والاتصالات بحسب المعايير الدولية المقبولة بهذا الشأن مثل(27001/2IEC ISO)	جميع المعلومات والتقنية المصاحبة لها
امن بيانات بطاقات الدفع وحمايتها	اعتماد القواعد والمعايير اللازمة لضمان متطلبات الحماية، والسرية والمصداقية والتوافرية والامتثال بطاقات الدفع - لإدارة أمن البيانات من قبل جميع الكيانات المشاركة في معالجة وإدارة بطاقات الدفع، بما ، والمجهزين، والمؤسسات المالية ومزودي خدمات الدفع الإلكتروني، فضلا عن جميع الكيانات الأخرى التي تقوم بتخزين، ومعالجة او نقل بيانات حامل البطاقة و/ أو بيانات التصديق الحساسة بحسب المعايير الدولية المعتمدة بهذا الشأن واتخاذ جميع	بطاقات الدفع الالكتروني

	الإجراءات الفعلية للحصول على شهادة PCI (DSS) وفقًا لتلك المعايير	
خطط استمرارية العمل للتعافي من الكوارث	وضع القواعد والمعايير اللازمة لبناء خطط التعافي من الكوارث وحماية الموظفين وخطط استمرارية الأعمال بما في ذلك اليات البناء والتشغيل والفحص والتدريب والتحديث على الخطط لضمان توافرية عمليات المؤسسة الحرجة	عمليات المؤسسة الحرجة وحماية البشر
إدارة مخاطر تقنية المعلومات	وضع القواعد والمعايير اللازمة لبناء مخاطر تقنية المعلومات والاتصالات بوصفها جزءا من المخاطر جميع عمليات الـ الكلية للمؤسسة، بما في ذلك حوكمة تلك المخاطر والمسؤوليات والمهام المناطة بالأطراف المختلفة، وآليات الخاصة بتقنية - تقييم وضبط ومراقبة المخاطر بهدف تعزيز عمليات اتخاذ القرار المبني على المخاطر وتحقيق أهداف المؤسسة	جميع عمليات المؤسسة ومدخلاتها الخاصة بتقنية المعلومات والاتصالات
امتثال تقنية المعلومات (Compliance IT)	وضع القواعد والمعايير اللازمة لضمان الامتثال لضوابط مصرف ليبيا المركزي والجهات الرقابية الأخرى، وللقوانين والانظمة السارية ولسياسات المؤسسة	جميع عمليات المؤسسة المعنية بموضوعات تقنية المعلومات والاتصالات

اسم السياسة	الغرض	النطاق
خصوصية البيانات (Data Privacy)	وضع القواعد والمعايير اللازمة الحماية البيانات الخاصة بالأشخاص الطبيعيين أو المعنويين من صابات الإفصاح والاستخدام غير المصرح به	البيانات الخاصة كافة
الاستعانة بخيرات خارجية(Outsourcing)	اعتماد سياسة عامة للاستعانة بالموارد بشكل عام وبموارد نقدية المعلومات والاتصالات بشمال خاص تلك الموارد سواء المؤسسة (In-sourcing) أو المملكة للغير (Outsourcing) تراعي الضوابط والانظمةوالأنظمة والقوانين وتحاكي أفضل الممارسات الدولية المقبولة بهذا الشان وتاخد بالحسبان العملية الإنتاجية (On-site Off-site Near site offshore) وتاخد بالحسبان وتراعي متطلبات مراقبة الخدمة (Service Levels)وتفعل حق االتدقيق Audit) (Right من قبل اطراف ثالثة محايدة موثوقة وتحقق متطلبات استمرارية العمل، وضوابط الحماية اللازمة لتلبية متطلبات السرية والمصداقية، فضلا عن متطلبات الكفاءة والفعالية في استغلال الموارد	عليات المؤسسة كافة
إدارة محفظة المشروع Management Portfolio project	وضع القواعد والمعايير اللازمة لإدارة المشاريع، بما في ذلك مراحل المشروع والحوكمة اللازمة التحقيق المتطلبات المتعلقة بالجودة Quality) .(Requirements وتلك المتعلقة بالحماية والسرية (Confidentiality Requirements)، وتلك المتعلقة بالامتثال تحقيقا لأهداف المؤسسة وعملياتها.	جميع مشاريع المؤسسة المتعلقة بتكنولوجيا المعلومات والاتصالات

مرفق رقم (6)

منظومة السياسات (حد أدنى)

إدارة الأصول **Asset Management**	وضع القواعد والمعايير اللازمة لتصنيف درجة مخاطر البيانات والأنظمة المختلفة وتحديد مالكيها وضوابط حمايتها مراحل دورة حياتها المختلفة.	البيانات والأجهزة والبرامج والأدوات المصاحبة لها.
الاستخدام المقبول لموارد تقنية المعلومات	وضع القواعد والمعايير اللازم لتحديد السلوك المقبول وغير المقبول لموارد تقنية المعلومات	الأجهزة والبرمجيات والتطبيقات والشبكات بما في ذلك الانترنت والبريد الالكتروني .
إدارة التغيير **Change Management**	وضع القواعد والمعايير اللازم لضمان مصداقية التغيير من حيث توثيق الموافقات اللازمة من مالكي الأصول الخاضعة للتغيير	جميع عمليات تكنولوجيا المعلومات والاتصالات
أجهزة الحواسيب الرئيسية **Servers**	وضع قواعد ومعايير لتقليل عمليات النقد والاستخدام غير المشروع للأجهزة بما في ذلك ضوابط نفاذ موظفي دائرة تقنية المعلومات وذوي الامتيازات العليا لبيانات التشغيل ، فضلاً عن معايير غدارة عمليات التشغيل اليومي للأجهزة البرمجيات المختلفة بما في ذلك ضوابط الحماية واليات المراقبة والصيانة الدورية لتلك الأجهزة .	جميع الحواسيب الرئيسية المملوكة أو المدارة من قبل المؤسسة لكل بيانات التطوير والفحص والتشغيل بما في ذلك نظم التشغيل والأدوات الأخرى المصاحبة لها.
أجهزة الكمبيوتر الطرفية	وضع قواعد ومعايير سلوكية وتقنية لضمان حماية البيانات الحساسة المخزنة على الأجهزة	كل الأجهزة الطرفية المرتبطة بالشبكات أو القائمة بحد ذاتها.
الأجهزة المحمولة	وضع قواعد ومعايير سلوكية وتقنية لضمان حماية البيانات الحساسة المخزنة على الأجهزة	كل الأجهزة المحمولة مثل Smart) ، PDA،Laptop،Memory،USB،Phone، Caeds..... Ete)

إدارة صلاحيات وامتيازات النفاذ Userr Access Management	وضع قواعد لضمان منح صلاحيات وامتيازات النفاذ للبيانات والبرامج والأجهزة لمستخدمها بحسب الحاجة للعمل وبالحد الادني بما يكفل السرية ، والمصداقية ، والتوافرية ، لموارد تفنية المعلومات والاتصالات	كل البرامج والأجهزة وقواعد البيانات وما هو في حكمها.

تطوير / اقتناء الأنظمة ةالبرمجيات System Development Life Cycle	وضع القواعد والمعايير اللازمة لتفيد مراحل تطوير / اقتناء الأنظمة والبرمجيات المختلفة لضمان تلبيها لمتطلبات العمل من خلال منهجيات التطوير المختلفة المتناسبة مع متطلبات العمل واهدافه	كل الاتفاقيات والتعاقدات والالتزامات مع الأطراف الخارجية والأطراف من داخل المؤسسة
إدارة مستوى الخدمة Service Level Management	وضع قواعد ومعايير لتحديد ومعايير لتحديد مستوى الخدمات المقدمة ، وقبولها ، وتوثيقها ، وقياسها ، ومراقبتها ن وتحسينها ، سواء من اطراف داخلية ام اطراف داخلية لضمان الاستغلال الأمثل للموارد ودعم عمليات المؤسسة المختلفة .	كل الاتفاقيات والتعاقدات والالتزامات مع الأطراف الخارجية والأطراف من داخل المؤسسة
النسخ الاحتياطي والاسترجاع Back – up and Rrstore	وضع قواعد ومعايير لأليات النسخ الاحتياطي والاسترجاع لضمان توافرية البيانات ومصداقيتها وسريتها	البيانات في بيانات التشغيل وحيثما يلزم
الاحتفاظ بالبيانات Data Retention	وضع قواعد ومعايير الخاصة بحجم البيانات الواجب توافرها سواء بشكل ورقي او تلك المتواجد على أجهزة الحواسيب والتطبيقات المختلفة والمدة الزمنية الواجب الاحتفاظ بها والمفاضلة بين حجم البيانات المتوافرة وسرعة الادجاء في الوصول الى البيانات	كل الأجهزة والبرمجيات ووسائل وأدوات الاحتفاظ بالبيانات
شراء الأنظمة والتجهيزات Purchasing Systems	وضع قواعد ومعايير للمفاضلة بين المؤردين الخارجين	كل التجهيزات التقنية والبرامج المتعلقة بها.

النفاذ عن بعد Remote Access	وضع قواعد ومعاير للربط الشبكي عن بعد بشبكات الحواسيب الخاصة بالمؤسسة لتقليل مخاطر الاطلاع والاستخدام لبيانات ومصادر المؤسسة الحساسة والأنظمة الضبط الداخلية المعنية بحماية أصول المؤسسة وللحماية من مخاطر	الأطراف والشركاء الداخليين والخارجيين مثل مزودي الخدمات ، ولجميع بيانات التطوير والفحص والتشغيل للأجهزة والشبكات ، ومنها على سبيل المثال لا الحصر شبكات الانترنت ، والشبكات المشفرة ، وخطوط الاتصال المختلفة مثل MPLS،VPN DSL، ISDB ،Frame relay

الشبكات Networks	وضع قواعد ومعايير لضمان تحقيق متطلبات الكفاءة والفعالية في استغلال عناصر الشبكات والاتصالات من جهة وتحقيق متطلبات الامن والحماية من جهة أخرى دعما لتحقيق اهداف المؤسسة	كل عاصر الشبكات بجميع البيانات
الشبكات اللاسلكية Wireless Networks	وضع قواعد ومعايير بغرض حماية البيانات الحساسية المتناقلة عبر الشبكات اللاسلكية من الاعتراض والاستخدام غير المشروع.	كل الشبكات اللاسلكية الفعلية منها والافتراضية
الجدران النارية Firewalls	وضع الحد الأدنى من القواعد والمعاير المنظمة لألية عمل أجهزة الجدران النارية ، والية حمايتها لتفعيلها بالشكل المطلوب والكفيل بحماية وضمان سرية مصداقية بيانات وعمليات المؤسسة وتوافريتها	العاملة بالبيانات كافة مثل (Firewalls) كل أجهزة DNS، Proxy, External ، DNS VPN Routers، Switches servers .... etc.
فحص الاختراق وتحليل التغيرات Penetrating Testing and Vulnerability Assessment	وضع قواعد ومعايير لفحص الأجهزة وعناصر الشبكات لضمان عدم وجود تغرات امنية تمكن من اختراق البيانات والأنظمة والعمليات الحساسة للمؤسسة .	كل أصول المؤسسة التقنية من أجهزة حواسيب رئيسية وحماية عناصر الشبكات والبرمجيات .
مقسم الهاتف الخاص Pravit Braanch Exchange	وضع الحد الادني من قواعد ومعايير الحماية لانظمة المقسم لضمان حماية والسرية لبيانات وعمليات المؤسسة من الاستخدام غير المشروع	كل اجهز المقسم المملوكة وغير المملوكة للمؤسسة .

مرفق رقم (7)

المعلومات والتقارير (حد أدني)

اسم التقرير	محتوياته
مصفوفة الصلاحيات والامتيازات Authority Matrix	مصفوفة تعدد الصلاحيات والامتيازات الممنوحة على جميع البرامج وقواعد البيانات وعناصر الشبكات مثل التفاصيل اسم المستخدم ووظيفته وصلاحيته او امتيازاته .
تحليل عوامل مخاطر تكنولوجيا المعلومات والاتصالات IT Risk Factors Analysis	1- التهديدات الداخلية . 2- التهديدات الخارجية 3- مواطن الضعف في إدارة موارد تقنية المعلومات والاتصالات . 4- مواطن الضعف في قدرة تقنية المعلومات والاتصالات على تمكين عمليات المؤسسة 5- مواطن الضعف في إدارة مخاطر تقنية المعلومات والاتصالات .
تحليل سيناريو مخاطر تكنولوجيا المعلومات والاتصالات IT Risk Scenario Analysis	1- مصدر التهديد اما داخلي او خارجي . 2- نوع التهديد (Threat Type) مثل الأخطاء او اختراق فيروس او احداث خارجية . 3- الحادث (Event) مثل الإفصاح عن معلومات سرية، او تعطيل، او تعديل غير مشروع او سرقة وتدمير او تصميم غير فعال للقوانين والأنظمة او الاستخدام غير المقبول. 4- الأصـــول المتأثرة (Asset or Resource Affected) مثل بشـــر او هياكل تنظيمه لعمليات البنية التحية لتقنية معلومات او معلومات برامج. 5- الوقت : وقت الحدوث، مدة الحادث ، عمر الحادث قبل اكتشافه.
سجل مخاطر تكنولوجيا المعلومات والاتصالات IT Risk Register	1- مقدمة: مالك لأصل ، فريق التقييم ، تاريخ التقييم الاحق ، ملخص تقييم المخاطر ، وخيار إدارة المخاطر. 2- سيناريو تحليل مخاطر تقنية المعلومات والاتصالات في أعلاه. 3- تقييم مخاطر تقنية المعلومات والاتصـالات من حيث احتسـاب محوري المخاطر متمثلة باحتمالية الحادث (Potentiality) وحجم الأثر (Impact or Severity) وبفضـل اسـتخدام مقياس معياري زوجي لمحاور التقييم ، واظهر حجم الأثر اسـتنادا الى اهداف وعمليات المؤسـسـة المتضـمنة تقنية المعلومات والاتصـالات باسـتخدام محاور التقييم لاحد النماذج المالية الاتية على سبيل المثال :

	أ- COBIT Information Criteria ب- COBIT For Risk ج- Balanced Scorecard (BSC) د- Extended BSC هـ- Westerman و- COSO ERM ز- FAIR (Factor Analysis of Information Risk) 4- قابلة تحمل المخاطر (Risk Appetite) . 5- خيار إدارة المخاطر (مقبول في حال كانت كمية المخاطر المحسوبة اقل من قابلية تحمل المخاطر) تخفيف ، تجنب ،تحويل). 6- بنود خطة إدارة المخاطر ومتابعتها (نفذت ، او قيد التنفيذ بحسب الخطة). 7- معايير أداء رئيسية لمراقبة مستوى المخاطر (نسبة الانحراف الموجب للقابلية تحمل المخاطر).

RACI Chart	قوائم تتضمن تحييد الجهة، او الجهات او الشخص او الأطراف المسئولة بشكل أولى (Responsible) وتلك المسؤولة بشكل نهائي (Accountable) ، وتلك المستشارة (Consulted) ، وتلك التي يتم اطلاعها (Informed)لكل عمليات إدارة موارد تقنية المعلومات والاتصالات وإدارة مخاطر وامن المعلومات والرقابة مستقلة.
ملف المخاطر IT Risk Profile	1- سجل المخاطر . 2- تحليل عوامل المخاطر . 3- الخسائر المتحققة وغير المحققة (Losses and Near - Misses) 4- تدقيق جهات مستقلة .
تقارير المخاطر IT Risk Report	يوضح كمية مخاطر تقنية المعلومات والاتصالات الحالية المتضمنة في عمليات المؤسسة ، والإجراءات المتخذة او التي سيتم اتخاذها لإدارة تلك المخاطر ، ويتم تصميم شكل عرض هذه التقارير بحيث تخدم متخذ القرار مالك العملية / لعمليات التي تقع ضمن مسؤوليته بحسب طلبه

خريطة المخاطر IT Risk Map or Heat map	رسم بياني يوضح 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 لها (Risk Appetite) ونسبة الانحراف الموجب على قابلية تحمل المخاطر (Risk Tolerance)
مؤشرات قياس المخاطر الرئيسية **Key Risk Indicators**	عبارة عن معايير قياس يتم تحديدها ومقارنتها بـــ (Benchmark) لمراقبة المخاطر الحالية للتأكد من عدم تجاوزها للقابلية على تحمل المخاطر ، ويتم تحديدها لتكون مؤشرات قياس رئيسية استنادا الى المعايير الاتية :- أ- الأثر : حصة وحجم المؤشر في قياس إثر المخاطر. ب- القابلية للقياس. ج- الاعتمادية . د- الحساسية
Risk Taxonomy	توضيح معاني المصطلحات المستخدمة في تعريف وقياس وإدارة ومراقبة المخاطر فضلا عم معايير قياس المخاطر والتعبير عنها بحيث يتم استخدام تلك المصطلحات بالمعني والمفهوم ذاتهما لدى جميع الشركاء ، وبما يتفق وضوابطنا بهذا الشأن.
Risk and control Activity Matrix (RCAM)	مصفوفة تبين كمية المخاطر المحسوبة والإجراءات والضوابط المقابلة المتخذة لإدارة تلك المخاطر ومدى كفايتها والسيطرة عليها.
موازنة امن المعلومات وحمايتها	يتم تحديد المصاريف المخطط لإنفاقها على امن المعلومات للعام القادم ضمن الموازنة العامة للمؤسسة وبما يتوافق والمشاريع المخطط لتنفيذها ، متضمنة تحليل الانحراف القائم لمصاريف العام الحالي مقارنة مع الموازنة المحددة للعام نفسه.
MIS Repot	مصفوفة تبين جميع أنواع التقارير المنتجة بحيث تظهر اسم مالك التقري ، ووظيفته ، ودورية انتاجه ، والاجراء المتخذ تجاهه.
استراتيجية او منهجية تدقيق تقنية المعلومات والاتصالات **Audit Strategy**	يتم تحديد اهداف تدقيق تقنية المعلومات والاتصالات ونطاق التدقيق وبرامج التدقيق المستخدمة في عمليات المراجعة .

ميثاق تدقيق تكنولوجيا المعلومات والاتصالات **IT Audit charter** **Engagement letter**	ميثاق مستقل او ضمن الميثاق العام للتدقيق الداخلي يتم فيه تحديد صلاحيات عمل تدقيق تكنولوجيا المعلومات والاتصالات ، ومسؤولياته ، وطبيعته ، ونطاقه ، وبما يتفق وضوابطنا بهذا الشأن ويتم تضمين الـــــــــــــ ( ) Engagement Letterالموقعة مع المدقق الخارجي بذلك أيضا.
خطة تدقيق تكنولوجيا المعلومات والاتصالات **IT Audit Plan**	يتم رسم خطة مستقبلية للتدقيق تكون مرتكزة ومبينة على المخاطر .
مصفوفة المؤهلات **HR Competencies**	تتضـــمن الشـــهادات الاكاديمية والمهنية والفنية ومجموع الخبرات والمهارات اللازم امتلاكها لكوادر إدارة تقنية المعلومات والاتصـــالات وإدارة مخاطر تقنية المعلومات والاتصـــالات ، والتشـــغيل وتدفيق تقنية المعلومات، والاتصالات، وامن المعلومات ،وحمايتها.
سجل تدقيق المعلومات والاتصالات Assurance Findings Register	يحتوي تقارير تدقيق تقنية المعلومات والاتصالات.
أفضل المعايير الدولية لإدارة موارد ومشاريع تقنية المعلومات والاتصالات وإدارة مخاطر تقنية المعلومات والاتصالات وامن وحماية والتدقيق على تقنية المعلومات والاتصالات	يتم انشـاء مكتبة بالمراجع المطلوبة بحسـب أفضـل الممارسـات الدولية وتوفير اسـتدامها لكادر المؤسـسـة بحسـب طبيعة العمل ، فضلا عن منظومة القوانين والأنظمة والضوابط المراعاة .

اسم الخدمة البرنامج الأداء	وصف
خدمات إدارة الحوادث Incident Management Services	مجموع الافراد والإجراءات والبرامج والأدوات المستخدمة في اكتشاف مخاطر وتقييمها واحتواء الحوادث ومعالجتها، والتصدي لها وكتابة التقارير حيالها ورفعها واغلاقها واستخلاص الدروس والعبر من خلال اليات المراجعة النافدة لها.
IT Assets Inventory	مجموع الافراد والإجراءات والبرامج والأدوات المستخدمة في عمليات جرد أصول تقنية المعلومات والاتصالات باستخدام حلول مثل:- - Configuration management database (CMDMB) . - Assetmangement systems. - Simple Network Management Protocol (SNMP). - Reporting agents.
النوعية بالممارسات السليمة لامن المعلومات	مجموع الافراد والإجراءات والبرامج والأدوات المستخدمة في تصميم رسائل دورية لكل من الشركاء الداخلين من كادر المؤسسة وللشركاء الخارجيين مثل زبائن المؤسسة لكيفية التعامل السليم لضمان الحد الأدنى من متطلبات امن المعلومات واستخدام أدوات ، مثل :- • Training courses (internal and external). • News feeds. • Knowledge bases (KBs). • Training tools. • Social media. • Email. • Collaboration. • Vendor and industry advisories. • CERT advisories.

مرفق رقم (8)

الخدمات والبرنامج والبيئة التحتية لتكنولوجيا المعلومات والاتصالات

اسم الخدمة ، البرنامج ، الأداء	وصف
امن وحماية البيانات والمعلومات المنطقي	مجموعة الافراد والإجراءات والبرنامج والأدوات المستخدمة في الحفاظ على سرية البيانات والمعلومات ومصداقيتها وتوافريتها واستخدام أدوات مثل :- • RKI sniffers DPI. • Encryption services. • Firewalls. • Packer analyzer sensors. • IPSL\IDS. • Data loss prevention (DLP). • System and device management solutions. • Software distribution solutions. • Remote management systems. • Virtualization and cloud management solutions. • Document management. • Data classification systems. • Application – centric data management solutions. • Data obfuscation solutions. • Vendor information security advisories and KBs. • Honeypots tarpits. • Antimalware anti rootkit antispyware antiphishing

مراقبة امن المعلومات	مجموع الافراد والإجراءات والبرنامج والأدوات المستخدمة لضمان توفير وسائل المراقبة المستمرة لتحقيق اهداف امن المعلومات وحمايتها مثل :- • Logs • SNMP • Alternating system • SIEM (Security Information and Event Management) • Management dashboards • Network operations centers (NOCs)
برمجيات تدقيق تكنولوجيا المعلومات والاتصالات	البرمجيات المساعدة في تدقيق تكنولوجيا المعلومات والاتصالات وكشف الاحتيال ، والبرمجيات المستخدمة في التخطيط وتقييم المخاطر ، وكتابة تقارير التحقيق وتوثيقها والنفاذ اليها مثل :- • CAATs (Computer Assisted Audit Techniques) • Document management system • Planning tool • Tracking issues system • Data analytics / sampling techniques • Workflow system

اسم الخدمة ، البرنامج ، الأداء	وصف
الاستضافة وضوابط الامن المادي والبيئي لغرف الخوادم الرئيسية وغرف الاتصالات والتزود بالكهرباء	توفير ضوابط الامن المادي والبيئي بالحد الأدنى بحسب ما يلي :- • يراعى تواجد الغرف وان تكون البيئة التحتية للبناية بعيدة في تصميمها ، ومحمية عن تهديدات فضائيات وتسربات المياه والصرف الصحي المحتملة ، سواء أسفل البناء ، او في نهايته بالقرب من الاسطح ، او أي مكان اخر معرض لذلك ، ويجب ان تكون مساحة الغرف كافية وتلبي احتياجات المؤسسة الحالية وتأخذ بالحسبان التوسع المستقبلي المحتمل. • يجب ان يكون مكان الغرف البناية بشكل عام غير محدود الوصول (سواء في طبيعة الموقع الجغرافي ام بموجب الاتفاقيات التعاقدية الحصرية) من قبل شركات الاتصالات كافة ومن مزودين متنوعين . • يجب أن تتمتع غرف الخوادم الرئيسية وغرف الاتصالات (مثل Routers, Switches ....etc) غرف تزويد الكهرباء بالحماية المادية والبيئة بحيث تكون محاطة بجدران مسلحة من شبابيك، ومعزولة من حيث التأثيرات الكهرومغناطيسية التي تؤثر سلبا في بيانات أجهزة الكمبيوتر ، ومخدومة بمدخل احتياطي محمكم لاستخدمه من قبل الافراد عدا الطوارئ، ويجب ان تكون الغرفة من حيث التصميم بمدخل الكهرباء وأجهزة مكافحة الحريق ، ويجب ان تحتوي على كواشف للدخان، والمياه والحرارة والرطوبة ، بدرجة حماية عالية ، ويجب أيضا توفير المراقبة التلفزيونية المسجلة، والتبريد الموزع على جميع مساحة الغرفة بشكل عادل ، لحماية الأجهزة من الحرارة والرطوبة المرتفعة ، مع توفير أجهزة

	لسحب الغبار من الغرفة ، وان يكون الدخول محكما ومراقبا بحيث يمنع غير المخولين من ذلك ، مع مراعاة عدم وضع اية إشارات تدل الغير على مكان تواجد تلك الغرف الحساسة في المؤسسة من دون مرافقين مخولين. • يجب تزويد غرف الخوادم وغرف الاتصالات بمداخل كهرباء متعددة والمصادر وان يكون التحويل بينها بشكل اوتوماتيكي ، أي توفير بطاريات (UPS) فضلا عمن مولدات كهرباء بالقدرة الكافية لتشغيل أجهزة وعمليات المؤسسة (الحساسة في الأقل) في حال انقطاع مصدر الكهرباء الرئيسي. • يجب الاخذ بالحسبان متطلبات الدفاع المدني ودائرة المواصفات والمقاييس (حيثما تطلب الامر ذلك). • كل ما ذكر انفا ، ينطبق أيضا على غرف الخوادم والاتصالات والكهرباء البديلة (Disaster Recovery Sites).

اسم الخدمة ، البرنامج ، الأداء	وصف
المعايير والمواصفات القياسية العالمية المعتمدة في انشاء مراكز البيانات (DATA CENTER)	• Uptime institute, TUI Tier Standard: Operational Sustainability. • ANSI/BICSI 002 Data Center Design and Implementation Best Practices. • CENELEC EN 50600 Information technology – Data center facilities and infrastructures. • CEELEC EN 50173 – 5 Information Technology – Generic Cabling systems • ISO/IEC 24764 information technology - Generic Cabling systems for Data Centers • ASHRAE 90.4 – 2016 – Environmental Conditions • ISO 9000 – Quality System • ISO 1400 – Environmental Management System • ISO 27001 - information Security • PCI – Payment Card Internet Exchange, Data Centre business continuity standard

للإعتبارات الفنية، يُسّمْح بِأستخدام اللّغة الإنجليزية لتلبية مُتَطلبات المُرفقات.

إنتهى ،،،