Republic Of Iraq

CENTRAL BANK OF IRAQ

جمهورية العراق

البنك المركزي العراقي

دائرة تقنية المعلومات والاتصالات

العدد : ١٤/٦١١

التاريخ : ٢٥/٤/٢٠١٩

NO :

Date :

الى / المصارف كافة

شركات مزودي خدمات الدفع الألكتروني المرخصة كافة

**م / ضوابط الحوكمة والادارة المؤسسية لتقنية المعلومات والاتصالات في القطاع المصرفي**

تحية طيبة ...

لغرض تعزيز وإدامة الإدارة المؤسسية الفعّالة والرشيدة لتقنية المعلومات والاتصالات وأمن المعلومات والتقنيات المصاحبة لها نرسل اليكم نسخة من:

**" ضوابط الحوكمة والإدارة المؤسسية لتقنية المعلومات والاتصالات في القطاع المصرفي"**

والتي تمثل إطار العمل لحوكمة وإدارة المعلومات والتقنية المصاحبة لها والمبادئ التوجيهية لإدارة مخاطر تقنية المعلومات والاتصالات وأمن البيانات والأمن السيبراني لدى المصارف والمؤسسات المالية الخاضعة لرقابة البنك المركزي العراقي.

**لإتخاذ الاجراءات الكفيلة بإعتماد وتطبيق هذه الوثيقة في مؤسساتكم ، مع التقدير.**

المرفقات://

- نسخة من ضوابط الحوكمة والإدارة المؤسسية لتقنية المعلومات والاتصالات في القطاع المصرفي

علي محسن إسماعيل

المحافظ وكالة

البنك المركزي العراقي

CBI
CENTRAL BANK OF IRAQ
1947

دائرة تقنية المعلومات والاتصالات
ICT Department

# ضوابط الحوكمة والإدارة المؤسسية لتقنية المعلومات والاتصالات في القطاع المصرفي

((حوكمة وإدارة المعلومات والتقنية المصاحبة لها والمبادئ التوجيهية لإدارة مخاطر تقنية المعلومات والاتصالات وأمن البيانات والأمن السيبراني لدى المصارف والمؤسسات المالية الخاضعة لرقابة البنك المركزي العراقي))

2019

أولًا: المقدمة

ثانيًا: نطاق وآلية التطبيق والأطراف المعنية

ثالثًا: أهداف ضوابط حوكمة وإدارة المعلومات والتقنية العامة

رابعًا: نشر ضوابط حوكمة وإدارة المعلومات والتقنية ذات الصلة

خامسًا: اللجان

سادسًا: التدقيق الداخلي والخارجي

سابعًا: الإطار العام لإدارة مخاطر تقنية المعلومات والاتصالات

ثامنًا: ضوابط حوكمة وإدارة المعلومات والتقنية ذات الصلة

تاسعًا: اقتناء وتطوير نظم المعلومات والاتصالات

عاشرًا: إدارة مشاريع تقنية المعلومات والاتصالات

الحادي عشر: إدارة خدمات تقنية المعلومات والاتصالات

الثاني عشر: موثوقية الأنظمة وتوافرها واسترجاعها

الثالث عشر: إدارة أمن البنية التحتية التشغيلية

الرابع عشر: حماية مراكز البيانات والرقابة عليها

الخامس عشر: الرقابة على الوصول للموارد

السادس عشر: الخدمات المالية عبر الإنترنت

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

# المصطلحات

| | |
|---|---|
| المؤسسة المالية | أي من المصارف وشركات مزوّدي خدمات الدفع الإلكتروني وشركات الصرافة والشركات المساهمة العامة أو المساهمة الخاصة المُرخّص لها بمزاولة خدمات الدفع أوإدارة وتشغيل أنظمة الدفع الإلكتروني |
| المجلس | مجلس إدارة المؤسسة وما في حكمه |
| الإدارة التنفيذية العليا | تشمل مدير عام المؤسسة أو المدير الإقليمي ونائب المدير العام أو نائب المدير الإقليمي ومساعد المدير العام أو مساعد المدير الإقليمي والمدير المالي ومدير العمليات ومدير إدارة المخاطر ومدير الخزينة (الاستثمار) ومدير الامتثال، فضلًا عن أيّ موظف في المؤسسة له سلطة تنفيذية موازية لأيٍّ من السلطات، أي: من المذكورين، ويرتبط وظيفيًّا مباشرة بالمدير العام. |
| بيئة تقنية المعلومات والاتصالات | هي مجموعة التجهيزات الحاسوبية الخاصة بالشبكات الداخلية والشبكات الخارجية والخوادم الرئيسة والبرمجيات العاملة عليها وجميع الأجهزة المساندة لها في الموقع الرئيس والبديل. |
| المعلومات (Information) | أيّة بيانات شفوية أو مكتوبة أو سجلات أو إحصاءات أو وثائق مكتوبة أو مصورة أو مسجلة أو مخزنة إلكترونيًّا، أو بأيّة طريقة أخرى تُعدُّ ذات قيمة للمؤسسة. |
| البيانات (Data) | الحقائق الخام ويمكن توضيحها بالحروف والأرقام التي من الممكن أن تمثل الأشخاص أو الأشياء أو الأحداث. |
| أصول المعلومات (Information Assets) | أيّة معلومات أو ملفات إلكترونية أو غير إلكترونية أو أجهزة أو وسائط تخزين أو برامج أو أيٍّ من مكونات بيئة تقنية المعلومات والاتصالات المُتعلِّقة بأعمال المؤسسة. |
| الهجوم السيبراني (Cyber Attack) | أيّة محاولة تدمير أو كشف أو تغيير أو تعطيل أو سرقة أو محاولة استغلال نقط ضعف أو نفاذ غير مشروع لأصول معلومات المؤسسة ضمن الفضاء السيبراني |
| الأمن السيبراني (Cyber Security) | الحفاظ على سرية وتكاملية وتوافرية المعلومات وأصول المعلومات التابعة للمؤسسة ضمن الفضاء السيبراني من أيّ تهديد سيبراني، عن طريق مجموعة من الوسائل والسياسات والضوابط وأفضل الممارسات بهذا الشأن. |
| التهديد السيبراني (Cyber Threat) | ظرف أو حدث يُحتمَل أن يستغل (عن قصد أو غير قصد) واحدة أو أكثر من نقط الضعف الموجودة في بيئة تقنية المعلومات والاتصالات للمؤسسة، ممّا يؤثر في أمنها السيبراني. |
| الحدث السيبراني (Cyber event) | أيّة واقعة تدلّ على وجود تهديد سيبراني على بيئة تقنية المعلومات والاتصالات للمؤسسة. |
| المخاطر السيبرانية (Cyber Risk) | مقدار ترجيح ناتج عن احتمال وقوع حدث سيبراني في نطاق أصول المعلومات للمؤسسة، وأثر ذلك الحدث في المؤسسة. |
| الحوكمة السيبرانية (Cyber Governance) | ترتيبات المؤسسة لوضع وتنفيذ ومراجعة نهجها لإدارة المخاطر السيبرانية |
| إدارة المخاطر السيبرانية ( Cyber Security Management) | عمليات تحديد وقياس وضبط ومراقبة المخاطر السيبرانية. |
| حوكمة البيانات (Data Governance) | هي عملية إدارة توافرية البيانات المستخدمة في المؤسسة، وأمنها، وسهولة استخدامها، وسلامتها. |
| الشيفرات الخبيثة (Malicious Code) | برمجيات أو ملفات ضارة تتضمن وظائف لها قدرات تؤثر بشكل سلبي، سواء بشكل مباشر أم غير مباشر، في بيئة تقنية المعلومات والاتصالات |

| | |
|---|---|
| الحماية (Protection) | توظيف الإجراءات والضوابط والتدابير الملائمة لتقديم خدمات وأعمال المؤسسة بصورة موثوقة |
| الكشف (Detection) | توظيف الضوابط والإجراءات المناسبة من أجل العلم بوقوع الحدث السيبراني فورًا |
| الاستجابة (Response) | توظيف الضوابط والإجراءات المناسبة لاحتواء الحدث السيبراني عند كشفه |
| الاستعادة (Restore) | عملية استرجاع المعلومات المُخزَّنة على وسائط النسخ الاحتياطية، عند تلف أو فقدان المعلومات الأصلية، أو الحاجة إليها بعد مدة من الزمن لإعادة سير عمل المؤسسة |
| التعافي (Recovery) | مجموعة الإجراءات التي يتمّ اتخاذها واتباعها لإعادة الأعمال في المؤسسة إلى وضعها الطبيعي، وإعادة تشغيل موارد التقنية المعتمدة في تشغيل عمليات المؤسسة إلى ما كانت عليه قبل وقوع الحدث |
| نقط الضعف (Vulnerabilities) | خلل أو نقص في ضوابط الحماية المستخدمة في أيّ من مكونات بيئة تقنية المعلومات والاتصالات المُتعلِّقة بأعمال المؤسسة الممكن استغلالها في عمليات الاختراق والهجوم السيبراني |
| ضوابط الوصول/النفاذ (Access Control) | القواعد والآليات المستخدمة للسماح باستخدام أصول المعلومات، ونفاذ الأشخاص المخوّلين فقط إليها، وبما يتوافق وطبيعة مسؤولياتهم في المؤسسة |
| الامتيازات والصلاحيات (Privileges) | مستوى الصلاحيات التي يتمّ منحها للمستخدمين للوصول للنفاذ واستخدام أيّ من مكونات بيئة تقنية المعلومات والاتصالات في المؤسسة |
| إدارة التغيير (Change Management) | إدارة وضبط وتوثيق أيّ تغيير يتمّ إجراؤه على أيّ من مكونات بيئة تقنية المعلومات والاتصالات في المؤسسة، أو أيّ تغيير في الإجراءات المعمول بها في المؤسسة من قبل الأطراف المخولة بالموافقة |
| تصنيف المعلومات | تحديد مستوى الحسّاسية المناسب للمعلومات التي يتمّ إنشاؤها أو تغييرها أو نقلها أو تعديلها أو حفظها على أية وسائل كانت وبأية تقنيات ممكنة، استنادًا إلى المخاطر المترتبة على الاطلاع والاستخدام غير المشروع لتلك المعلومات |
| السرية (Confidentiality) | حماية المعلومات من عمليات الاطلاع والنشر والإفصاح والاستخدام غير المشروع |
| التوافرية (Availability) | إمكانية استخدام والوصول/ النفاذ إلى المعلومات والأنظمة في المؤسسة واسترجاعها عند الطلب |
| التكاملية (Integrity) | دقة واكتمال وسلامة المعلومات أو نظم المعلومات، أو أيّ جزء منها والتحقّق من أنّه لم تطرأ عليها أيّة زيادة أو نقصان أو تغيير غير مشروع |
| الملاءمة (Appropriate) | توافر الحد الأدنى من المتطلبات لأعضاء مجلس إدارة المصرف، وهيأة الرقابة الشرعية في المصرف الإسلامي وأعضاء الإدارة التنفيذية |
| الإدارة التنفيذية ( Executive Management) | الموظفون الرفيعو المستوى كما ورد ذلك في المادة (1) من قانون المصارف رقم (94) لسنة 2004، وتوافقًا مع تعليمات البنك المركزي العراقي والهيكل التنظيمي للمصرف |
| المبادئ التوجيهية (Guidelines) | عبارة عن قائمة بأفضل الممارسات في القطاع المصرفي التي من المتوقع أن تعتمدها المؤسسة. |

| | |
|---|---|
| زمن التعافي المستهدف (Recovery Time Objective) RTO | أقصى وقت مسموح به لإعادة تشغيل الخدمة أو العملية بعد حدوث الانقطاع الخدمات تقنية المعلومات والاتصالات |
| نقطة الاسترجاع المستهدفة (Recovery Point Objective) RPO | هو العمر الأقصى المسموح للبيانات التي قد تُفقَد عند استعادة الخدمة، بعد حدوث انقطاع. |
| العمليات الحرجة (Critical Operations) | العمليات التي لا يمكن تحمُّل توقفها لمدد زمنية طويلة بحسب دراسات تحليل الأثر على الأعمال في المؤسسة، وتلك العمليات ذات المخاطر والأهمية النسبية للمؤسسة |
| البريد الإلكتروني (E-mail) | الخدمة التي يمكن توفيرها للمستخدمين من إنشاء وإرسال واستقبال وتخزين الرسائل الإلكترونية باستخدام أنظمة الاتصالات الإلكترونية |
| التشفير (Encryption) | عملية تحويل المعلومات إلى شكل غير مقروء أو مفهوم. |
| الطرف الثالث (Third Party) | الجهة التي تعهد إليها المؤسسة تولي الأعمال الفنية والتقنية بشكل كلي أو جزئي؛ لمساعدتها على القيام بالأعمال المُرخَّصة بها، بما لا يتعارض وأحكام التشريعات النافذة |
| الاسناد الخارجي (Outsourcing) | الاستعانة بطرف ثالث أو توظيف موارده؛ لتسيير أعمال المؤسسة أو جزء من أعمالها التي تقع ضمن مسؤوليتها |
| الأمن المادي (Physical Security) | معايير وإجراءات الحماية التي تراقب أو تحدد الدخول إلى أيّ من مرافق المؤسّسة، أو مواردها، أو معلومات المؤسسة المُخزَّنة على وسائط : فيزيائية لمنع الوصول إلى الموارد المعلوماتية والأنظمة، مثل المباني وخزائن الملفات والأجهزة المكتبية والمحمولة والخوادم والمُعدّات |
| أصحاب المصالح (Stakeholders) | أي ذي مصلحة في المؤسسة، مثل المساهمين أو الموظفين أو الدائنين أو الزبائن أو المزوّدين الخارجيين أو الجهات الرقابية المعنية |
| سجلات الأحداث (Event log) | ملفات بيانات الأحداث الأمنية والتشغيلية التي تنتج عن مكونات النظام لفهم نشاط النظام وتشخيص المشاكل التي قد تحصل عليه |
| سجلات التدقيق (Audit Trail) | ملفات بيانات تقدم أدلة مستندية على تسلسل العمليات الوظائفية والإدارية التي تحدث على الأنظمة |
| تقييم المخاطر (Risk Assessment) | قياس وتحديد احتمالية حدوث المخاطر وشدتها وتوقع مقدار تأثيرها في المؤسسة |
| اختبارات الاختراق (Penetration Testing) | اختبار يحاول فيه المختصون البحث عن الثغرات الأمنية والتحايل على الخصائص الأمنية لأنظمة المعلومات والضوابط الأمنية واستغلالها لمحاولة اختراق تلك الأنظمة من خارج أو داخل المؤسسة؛ لمعرفة مدى فعالية الضوابط الأمنية المستخدمة من قبل المؤسسة لحماية أنظمتها |
| الوصول عن بعد (Remote Access) | تمكين الاتصال مع أنظمة المؤسسة من خارج الشبكة الداخلية الخاصّة بها، سواء كان ذلك التمكين لغايات عمل موظفيها عن بعد، أم لتأمين الاتصال مع شركاء العمل، أو من قبل طرف ثالث. |
| DAS<br>DIRECT ATTACHED STORAGE | هي وسيلة التخزين الرقمي المتصلة مباشر بالكومبيوتر مثل محركات الأقراص الصلبة والأقراص الثابتة ومحركات الأقراص الضوئية. |
| NAS<br>NETWORK ATTACHED STORAGE | هو وحدة التخزين الشبكي لتخزين بيانات الكمبيوتر على الشبكة لتوفير الوصول إليها لأكبر عدد ممكن من أجهزة المستخدمين الأخرى، أو الزبائن المتصلة بالشبكة نفسها |
| SAN<br>STORAGE AREA NETWORK | هي نظام تخزين مخصص عالي الأداء يقوم بنقل بيانات مستوى الكتلة بين الخوادم وأجهزة التخزين، عادةً ما يتمّ استخدام SAN في مراكز البيانات أو المؤسسات أو بيئات الحوسبة الافتراضية |

## أولًا: المقدمة

أدى تطور تقنية المعلومات والاتصالات إلى تغييرات سريعة في الطريقة التي تتم بها الأعمال والعمليات في القطاعات المصرفية، ولم تعُدْ تقنية المعلومات والاتصالات وظيفة دعم داخل المؤسسات المالية فقط، بل أصبحت عامل تمكين أساس لاستراتيجيات الأعمال، بما في ذلك الوصول إلى احتياجات الزبائن وتلبية احتياجاتهم. من خلال توفير وإدامة الخدمات التقنية وفقًا لأنسب المعايير الدولية، وأفضل الممارسات للحفاظ على جودة المعلومات، من خلال مواكبة التطورات التقنية وتنمية قدرات ومهارات الموارد البشرية، وبشكل يؤدي إلى تحقيق أهداف البنك المركزي الواردة في قانون البنك المركزي 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 متنوعة من المنتجات والخدمات أن تعمل بأنظمتها المالية في مواقع متعددة وبدعم من مختلف مقدمي الخدمات.

وتواجه المؤسسات المالية أيضًا التحدي المتمثل في مواكبة احتياجات وتفضيلات المستهلكين الذين يكتسبون مزيدًا من الخبرة في مجال تقنية المعلومات والاتصالات نظرًا إلى سرعة وسهولة استخدام الإنترنت والأجهزة المحمولة للحصول على الخدمات المالية وتقوم المؤسسات المالية بشكل متزايد بنشر المزيد من التقنية المتقدمة والأنظمة عبر الإنترنت، بما في ذلك الأنظمة المصرفية عبر الإنترنت والخدمات المصرفية عبر الهاتف المحمول، وأنظمة الدفع، ومنصات التداول عبر الإنترنت، وبوابات التأمين للوصول إلى زبائنها. وفي هذا الصدد يجب أن تفهم المؤسسات المالية بشكل كامل حجم وكثافة مخاطر التقنية من هذه الأنظمة. كما يجب أن تضع أنظمة إدارة مخاطر كافية وقوية، فضلًا عن عمليات تشغيل لإدارة مثل هذه المخاطر.

تُحدّد المبادئ التوجيهية لإدارة المخاطر التقنية (المبادئ التوجيهية) الواردة في COBIT والمعيار الدولي ISO 31000 مبادئ إدارة المخاطر وأفضل الممارسات لتوجيه المؤسسات المالية في ما يأتي:

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

إنّ درجة التقيد بهذه المبادئ من قبل مؤسسة ما سيُعتمَد من قبل البنك المركزي معيارًا لتقييم مخاطر هذه المؤسسة.

**ثانيًا: نطاق وآلية التطبيق والأطراف المعنية**

على جميع المصارف وشركات الدفع الإلكتروني وفروع المصارف الأجنبية العاملة في العراق الالتزام بهذه الضوابط بالقدر الذي ينطبق عليها، أو بدليل وسياسات الحوكمة وإدارة تقنية المعلومات والاتصالات ذات الصلة الصادرة عن الإدارة العامّة، أو السلطة الرقابية في الدولة، أيهما أكثر تحقيقا لأهداف ضوابطنا، وفي حال كانت هذه الأخيرة هي الأكثر تحقيقًا، فإن على المؤسسات تقديم ما يؤيد ذلك إلى البنك المركزي، مع مراعاة عدم التعارض مع التشريعات، وفي حال وجود تعارض فعلى المؤسسات إعلام الإدارة العامّة للبنك المركزي، بذلك وتقديم التوضيح اللازم لهذا التعارض والحصول على موافقة البنك المركزي على أُسلوب معالجة هذا التعارض.

وعلى المصارف عقد اتفاقيات إسناد (outsourcing) مع المصادر الخارجية لتوفير الموارد البشرية والخدمات والبنى التحتية لتقنية المعلومات والاتصالات بهدف تسيير عمليات المؤسسة والتأكد من التزام المصادر الخارجية بتطبيق بنود هذه الضوابط بشكل كلي أو جزئي بالقدر الذي يتناسب وأهمية وطبيعة عمليات المؤسسة، والخدمات، والبرامج، والبنية التحتية المُقدَّمة قبل وأثناء مدّة التعاقد، وبما لا يعفي المجلس والإدارة التنفيذية العليا من المسؤولية النهائية لتحقيق متطلبات الضوابط بما في ذلك متطلبات التدقيق الواردة في المادة (7)، وتُعدُّ مدّة نفاذ الضوابط أو مدّة التعاقد المدة الزمنية الواجب خلالها توفيق أوضاع الشركات المتعاقد معها حاليًا، ولا سيّما أيهما أسبق.

يشمل نطاق تطبيق الضوابط كافّةً عمليات المؤسسة المرتكزة على تقنية المعلومات والاتصالات بمختلف الفروع والإدارات، وتُعدُّ جميع الأطراف أصحاب المصالح معنيّة بتطبيق الضوابط كُلّ بحسب وظيفته وموقعه، ولتسهيل عملية التطبيق يتمّ 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 ومسؤوليتها الرئيسة بهذا الشأن:

1. رئيس وأعضاء المجلس والخبراء الخارجين المُستعان بهم: تولّي مسؤوليات التوجيه العام للمشروع/ البرنامج والموافقة على المهام والمسؤوليات ضمن المشروع، والدعم وتقديم التمويل اللازم.
2. المدير العام ونوّابه ومساعدوه، ومديرو العمليات والفروع: تولّي مسؤليات تسمية الأشخاص المناسبين من ذوي الخبرة بعمليات المؤسسة لتمثيلهم في المشروع وتوصيف مهامهم ومسؤلياتهم.
3. مدير ولجان تقنية المعلومات والاتصالات التوجيهية ومديرو المشاريع: تولّي مسؤليات إدارة المشروع/ البرنامج وتوجيهه والإشراف عليه بشكل مباشر، والتوصية بتوفير الموارد اللازمة لإتمامه، والتأكد من الفهم الصحيح من قبل الأطراف كافّةً بمتطلبات وأهداف الضوابط المحددة في هذا الدليل.
4. التدقيق الداخلي: تولّي مسؤلياته المناطة به بموجب هذه الضوابط بشكل مباشر والتوصية بتوفير المعلومات اللازمة لإتمامه، والتأكد من الفهم الصحيح من قبل الأطراف كافّةً بمتطلبات وأهداف الضوابط المُحدَّدة في هذا الدليل.
5. إدارة المخاطر، وأمن المعلومات، والامتثال، والقانونية: تولّي مسؤليات المشاركة في المشروع/ البرنامج بما يمثل دور تلك الإدارات، والتأكد من تمثيل المشروع/ البرنامج من قبل الأطراف المعنية كافّةً.
6. المتخصصون وحملة الشهادات الفنية والمهنية الخاصة بأفضل الممارسات ( COBIT Assessor, Implementation, COBIT Foundation, CGEIT) المُستعان بهم من داخل المؤسسة ومن خارجها: تولّي مَهمّة المرشد لنشر المعرفة بالمعيار وتسهيل عملية التطبيق.

على المصارف تحديد إطار زمني وخطة عمل خلال ستة أشهر وفقًا لهذه الضوابط على أن تتضمن هذه الخطة الموازنات اللاحقة التي تضمن تطبيق هذه الضوابط، والوصول إلى مستوى نضوج (3.2) ( Deployment maturity level 3.2: Established) بعد ثمانية عشر شهرا بحد أقصى من تاريخها للعمليات الأساسية المُتعلّقة بتقنية المعلومات والاتصالات، والوصول لمستوى نضوج (5.2) (maturity level 5.2: Optimization) خلال ستة وثلاثين شهرًا، حدًّا أقصى من تاريخها، وبشكل كامل لجميع الأعمال المُتعلّقة بتقنية المعلومات والاتصالات، على أن تتمّ مراجعة مستوى النضوج للأعمال غير المُتعلّقة بتقنية المعلومات والاتصالات وفقًا لخطة العمل التي اعتمدتها المؤسسة، والوصول إلى نضوج (5.2) بمدّة لا تتجاوز خمس سنوات لجميع الأعمال المُتعلّقة وغير المُتعلّقة بتقنية المعلومات والاتصالات.
يُعدُّ تطبيق متطلبات التعليمات خطوة أولى ونقطة شروع وبداية باتجاه التطوير والتحسين المستمرين لحوكمة المعلومات وإدارتها، والتقنية المصاحبة لها، وعليه يتوجب على إدارات المصارف مواكبة الإصدارات الناشئة المستقبلية وتحديثاتها فيما

يخص الإطار العام الذي تمّ الاستناد إليه عند صياغة هذه الضوابط (COBIT)، وما يحتويه من معايير دولية أخرى مساندة لها ضمن هذا الإطار.

ولا بُدّ عند التطبيق والدخول في تفاصيل الركائز (الدعامات) السبعة، والعمليات، والأهداف الفرعية، أن تقوم المصارف بتطويع (Tailoring) كُلّ ذلك بما ينسجم ومعطيات كُلّ مصرف على حِدَة، في سبيل خدمة أهداف ومتطلبات الضوابط والمعيار (COBIT)، والعمل على إيجاد التغيير المطلوب لتوفير وتهيئة البيئة اللازمة للتطبيق.
واتباع اسلوب تحليل الانحراف (GAP Analysis) بين الوضع الحالي، والمقارنة مع متطلبات الضوابط والمعيار تمهيدًا لعملية التطبيق.
وعلى المصارف إرسال تقارير الإجاز المُتعلِّقة بالامتثال لتحقيق متطلبات ضوابط البنك المركزي العراقي كُلّ ستة أشهر من تاريخ الضوابط، موضحةً فيها مستوى الإجاز لكل بند من بنود الضوابط للعمليات المُتعلِّقة وغير المُتعلِّقة بتقنية المعلومات والاتصالات الاتصالات.

**ثالثًا: أهداف ضوابط حوكمة تقنية المعلومات والاتصالات في القطاع المصرفي العراقي**

وتُعدُّ الأهداف وعمليات دليل حوكمة تقنية المعلومات والاتصالات بحسب المرفقين (2) و(3) على الترتيب، ومعطياتها حدًّا أدنى يتوجب على إدارة المؤسسة العليا الامتثال لها وتحقيقها بشكل مستمر، وتُعدُّ اللجنة التوجيهية لتقنية المعلومات والاتصالات المسؤول الأوّل عن ضمان الامتثال بتحقيق متطلباتها، ولجنة حوكمة تقنية المعلومات والاتصالات والمجلس بصورة كُلية، هي المسؤول النهائي بهذا الشأن، ويتوجب على دوائر المؤسسة كافّةً، وبصورة خاصة دائرة تقنية المعلومات والاتصالات وإدارة أمن المعلومات وإدارة المشاريع تحديد عملياتها وإعادة صياغتها، بحيث تحاكي وتغطي متطلبات جميع عمليات حوكمة تقنية المعلومات والاتصالات الواردة في المرفق رقم (3).

يتولّى المجلس المسؤوليات المباشرة لعمليات التقييم والتوجيه والرقابة، فضلًا عن مسؤوليته المباشرة عن عملية ضمان إدارة حصيفة لمخاطر تقنية المعلومات والاتصالات وعملية إدارة المخاطر الواردة في المرفق رقم (3) على الترتيب، بالتعاون مع دائرة إدارة المخاطر في المؤسسة، إذ تهدف هذه الضوابط إلى تلبية احتياجات أصحاب المصالح ( Stakeholder's Needs) وتحقيق توجيهات وأهداف المؤسسة من خلال تحقيق أهداف تقنية المعلومات والاتصالات، وبما يضمن:

1. توفير معلومات ذات جودة عالية تكون مرتكزًا بدعم آليات صنع القرار في المؤسسة.
2. إدارة حصيفة لموارد ومشاريع تقنية المعلومات والاتصالات للإفادة من تلك الموارد، وتقليل الهدر فيها.
3. توفير بنية تحتية لتقنية متميزة وداعمة تُمكِّن المؤسسة من تحقيق أهدافها.
4. الارتقاء بعمليات المؤسسة المختلفة من خلال توظيف منظومة تقنية كفوءة وذات اعتمادية متميزة.
5. إدارة حصيفة لمخاطر تقنية المعلومات والاتصالات تكفل الحماية اللازمة لموجودات المؤسسة.
6. المساعدة في تحقيق الامتثال لمتطلبات القوانين والتشريعات والضوابط، فضلًا عن الامتثال لاستراتيجية وسياسات وإجراءات العمل الداخلية.
7. تحسين نظام الرقابة الداخلي.
8. تحسين مستوى الرضا عن تقنية المعلومات والاتصالات من قبل مستخدميها بتلبية احتياجات العمل بكفاءة وفعالية.
9. إدارة خدمات الأطراف الخارجية المُوكَل إليها تنفيذ عمليات ومهام الخدمات والمنتجات المُتعلِّقة بتقنية المعلومات والاتصالات.

تبنّي أفضل المعايير الدولية والممارسات وقواعد العمل والتنظيم، مثل: [ ISO 27000، COBIT BASEL، مكتبة البنية التحتية لتقنية المعلومات والاتصالات ](ISO20000) (ITIL)، نقطةَ انطلاق يتمّ الارتكاز والبناء عليها في مجالي حوكمة وإدارة عمليات ومشاريع وموارد تقنية المعلومات والاتصالات.

فصل عمليات ومهام ومسؤوليات المجلس في مجال الحوكمة عن تلك التي تقع ضمن حدود مسؤولية 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 مستمر.

**رابعًا: نشر ضوابط حوكمة وإدارة المعلومات والتقنية ذات الصلة**

على كُلّ مصرف نشر إجراءاته المتخذة فيما يخص دليل حوكمة تقنية المعلومات والاتصالات، وبأية طريقة أخرى مناسبة لإطلاع الجمهور، وعلى المؤسسة الإفصاح في تقريرها السنوي عن وجود دليل خاص لحوكمة وإدارة المعلومات والتقنية المصاحبة لها، أو متضمن لدليل الحوكمة المؤسسية لديه، وعن مدى التزامه بتطبيق ما جاء فيه.

**خامسًا: اللجان**

**أ. لجنة حوكمة تقنية المعلومات والاتصالات**

على المجلس تشكيل لجنة حوكمة تقنية المعلومات والاتصالات وتتشكّل هذه اللجنة من ثلاثة أعضاء في الأقل، ويُفضّل أن تضمّ في عضويتها أشخاصًا من ذوي الخبرة أو المعرفة الاستراتيجية في تقنية المعلومات والاتصالات وللجنة الاستعانة عند اللزوم وعلى نفقة المؤسسة بخبراء خارجيين وذلك بالتنسيق مع رئيس المجلس، لغرض تعويض النقص في هذا المجال من جهة، ولتعزيز الرأي الموضوعي من جهة أخرى، وللجنة دعوة أيّ من إداريي المؤسسة لحضور اجتماعاتها؛ للاستعانة برأيهم بمافيهم المعنيين في التدقيق الداخلي وأعضاء الإدارة التنفيذية العليا (مثل مدير تقنية المعلومات والاتصالات) أو المعنيين في التدقيق الخارجي، ويُحدّد المجلس أهدافها ويفوّضها بصلاحيات من قبله، وذلك وفق ميثاق يوضح ذلك، على أن تقوم برفع تقارير دورية للمجلس، علمًا أنّ تفويض المجلس صلاحيات للجنة أو أيّة لجنة أخرى لا يعفيه بصورة كلية من تحمُّل مسؤولياته بهذا الشأن، وتجتمع اللجنة بشكل دوري (ثلاثة أشهر في الأقل)، وتحتفظ بمحاضر اجتماعات موثقة، وتتولى المهام الآتية:

1. اعتماد الخطط الاستراتيجية لتقنية المعلومات والاتصالات والهياكل التنظيمية المناسبة بما في ذلك اللجان التوجيهية على مستوى الإدارة التنفيذية العليا وبصورة خاصة (اللجنة التوجيهية لتقنية المعلومات والاتصالات)، وبما يضمن تحقيق الأهداف الاستراتيجية للمؤسسة وتلبيتها، وتحقيق أفضل قيمة مضافة من مشاريع واستثمارات موارد تقنية المعلومات والاتصالات، واستخدام الأدوات والمعايير اللازمة لمراقبة والتأكد من مدى تحقق ذلك، مثل استخدام نظام بطاقات الأداء المتوازن لتقنية المعلومات والاتصالات ( IT Balanced Scorecards) واحتساب مُعدّل العائد على الاستثمار (ROI)، وقياس أثر المساهمة في زيادة الكفاءة المالية والتشغيلية.
2. اعتماد الإطار العام لإدارة وضبط ومراقبة موارد ومشاريع تقنية المعلومات والاتصالات يحاكي أفضل الممارسات الدولية المقبولة بهذا الشأن وعلى وجه التحديد (COBIT) ( Control Objective for Information and Related Technology) بجميع إصداراتها لتحقيق 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 تقنية المعلومات والاتصالات الواردة في المرفق رقم (3).
3. اعتماد مصفوفة الأهداف المؤسسية، الواردة في المرفق رقم (1)، وأهداف المعلومات والتقنية ذات الصلة، الواردة في المرفق رقم (2)، وعَدّ معطياتها حدًّا أدنى، وتوصيف الأهداف الفرعية اللازمة لتحقيقها.

4. اعتماد مصفوفة للمسؤوليات (RACI Chart) تجاه العمليات الرئيسة لحوكمة تقنية المعلومات والاتصالات في المرفق رقم (3)، والعمليات الفرعية المنبثقة عنها من حيث: الجهة أو الجهات أو الشخص أو الأطراف المسؤولة بشكل أولي Responsible، وتلك المسؤولة بشكل نهائي Accountable، والأطراف الاستشارية Consultant، وتلك التي يتمّ إطلاعها تجاه كُلّ العمليات Informed في المرفق المذكور بهذا الشأن.
5. التأكد من وجود إطارعام لإدارة مخاطر تقنية المعلومات والاتصالات يتوافق والإطار العام الكلي لإدارة المخاطر في المؤسسة ويتكامل معه، وفقًا للمعايير الدولية مثل (ISO 73، ISO 31000 ) ويأخذ بالحسبان جميع عمليات حوكمة تقنية المعلومات والاتصالات الواردة في المرفق رقم (3)، ويلبّيها.
6. اعتماد موازنة موارد ومشاريع تقنية المعلومات والاتصالات بما يتوافق والأهداف الاستراتيجية للمؤسسة.
7. الإشراف العام والاطلاع 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.

**ملحوظة: تدمج مهام لجنة حوكمة تقنية المعلومات والاتصالات مع مهام لجنة حوكمة المصارف مرحلةً أولى لمدة سنة - ثلاث سنوات بعد ذلك تنفصل اللجنة وتصبح لجنة حوكمة تقنية المعلومات والاتصالات منفصلة عن لجنة حوكمة المصارف.**

**ب. اللجنة التوجيهية لتقنية المعلومات والاتصالات:**

على الإدارة التنفيذية العليا تشكيل اللجنة التوجيهية لتقنية المعلومات والاتصالات لتحقيق الأهداف الاستراتيجية للمؤسسة وبشكل مستدام، وعليه يتمّ تشكيل لجنة تسمى باللجنة التوجيهية لتقنية المعلومات والاتصالات، برئاسة المدير العام والمديرين الفرعيين، بما في ذلك مدير تقنية المعلومات والاتصالات ومدير إدارة المخاطر ومدير أمن المعلومات، وينتخب المجلس أحد أعضائه ليكون عضوًا مراقبًا في هذه اللجنة، فضلًا عن مدير التدقيق الداخلي الذي تكون مهمته مراقبًا، وليس عضوًا في اللجنة، ويتمّ حضوره فقط حين تقديم أو مناقشة تقريره لتحقيق مبدأ الاستقلالية والموضوعية، ويمكنها دعوة الغير لدى الحاجة لحضور اجتماعاتها، وتوثيق اللجنة اجتماعاتها بمحاضر أُصولية، وتجتمع اللجنة التوجيهية دوريًا مرة كُلّ ربع سنوي في الأقل، وتتولى بصورة خاصة القيام بالمهام الآتية:

1. إعداد الخطط الاستراتيجية والتشغيلية لإدارة المخاطر الكفيلة بالوصول الى الأهداف الاستراتيجية المقررة من قبل المجلس، والإشراف على تنفيذها لضمان تحقيقها ومراقبة العوامل الداخلية والخارجية المؤثرة فيها بشكل مستمر.
2. ربط مصفوفة الأهداف المؤسسية بمصفوفة أهداف المعلومات والتقنية 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 تقنية المعلومات والاتصالات، الواردة في المرفقين (2) و(3) على الترتيب، حدًّا أدنى، والاستعانة بالعنصر البشري الكفوء والمناسب في المكان المناسب من خلال هياكل تنظيمية تشمل كُلّ العمليات اللازمة لدعم الأهداف التي تراعي فصل المهام، وعدم تضارب المصالح وتطويع البنية التحتية التقنية والخدمات الأُخرى المُتعلِّقة بها خدمةً للأهداف، وتولي عمليات الإشراف على سير تنفيذ مشاريع حوكمة تقنية المعلومات والاتصالات وعملياتها.
4. ترتيب مشاريع وبرامج تقنية المعلومات والاتصالات بحسب الأولوية.
5. مراقبة مستوى الخدمات الفنية والتقنية والعمل على رفع كفاءتها وتحسينها بشكل مستمر.
6. رفع التوصيات اللازمة للجنة حوكمة تقنية المعلومات والاتصالات بشأن الأُمور الآتية:

- تخصيص الموارد اللازمة والآليات الكفيلة بتحقيق مهام لجنة حوكمة تقنية المعلومات والاتصالات.
- أيّة انحرافات قد تؤثر سلبًا في تحقيق الأهداف الاستراتيجية.
- أيّة مخاطر غيرمقبولة مُتعلِّقة بتقنية المعلومات وأمنها وحمايتها.
- تقارير الأداء والامتثال بمتطلبات الإطار العام لإدارة وضبط ومراقبة موارد ومشاريع تقنية المعلومات والاتصالات.

7. تزويد لجنة حوكمة تقنية المعلومات والاتصالات بمحاضر اجتماعاتها أوّلًا بأول، والحصول على ما يفيد الاطلاع عليها.

**سادسًا: التدقيق الداخلي والخارجي**

مع زيادة تعقيد مخاطر تقنية المعلومات والاتصالات هناك حاجة متزايدة لتطوير نظم رقابة داخلية فعّالة لإدارة المخاطر التقنية.

توافر عمليات التدقيق في تقنية المعلومات والاتصالات لمجلس الإدارة والإدارة العليا تقييمًا مستقلًا وموضوعيًّا لإدارة المخاطر التقنية.

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

أ- على المجلس رصد الموازنات الكافية وتخصيص الأدوات والموارد اللازمة، بما في ذلك العنصر البشري المؤهَّل من خلال أقسام متخصصة بالتدقيق على تقنية المعلومات والاتصالات، والتأكد من أن كُلًّا من دائرة التدقيق الداخلي في المؤسسة والمُدقِّق الخارجي قادران على مراجعة عمليات توظيف موارد ومشاريع تقنية المعلومات والاتصالات وإدارتها وعمليات المؤسسة المرتكزة عليها، مراجعة فنية متخصصة (IT Audit)، وتدقيقها، بحسب البند (د) من هذه المادة، من خلال كوادر مهنية مؤهَّلة ومعتمدة دوليًّا في هذا المجال، حاصلين على شهادات اعتماد مهنية سارية مثل (CISA) من جمعيات دولية مؤهِّلة بموجب معايير الاعتماد الدولي للمؤسسات المانحة للشهادات المهنية (ISO/IEC 17024) و/أو أية معايير أُخرى موازية.

ب- على لجنة التدقيق المنبثقة عن المجلس من جهة، والمدقِّق الخارجي من جهة أُخرى، تزويد البنك المركزي العراقي بتقرير سنوي للتدقيق الداخلي، وآخر للتدقيق الخارجي على الترتيب يتضمن ردّ الإدارة التنفيذية واطلاع وتوصيات المجلس بشأنه، وذلك بحسب ما ورد في البند (د/2) من هذه المادة ووفقًا لأنموذج تقرير تدقيق (مخاطر- ضوابط) المعلومات والتقنية ذات الصلة في المرفق رقم (4)، وذلك خلال الربع الأوّل من كُلّ عام، وتحل هذه التقارير محل نظيرتها أو التي تشملها من التقارير المطلوبة بموجب ضوابط سابقة.

ج- على لجنة التدقيق تضمين مسؤوليات عمل تدقيق تقنية المعلومات والاتصالات وصلاحياته، ونطاقه، ضمن ميثاق التدقيق (Audit charter) من جهة، وضمن إجراءات متفق عليها مع المُدقِّق الخارجي من جهة أُخرى، وبما يتوافق وهذه الضوابط ويغطّيها.

د- على المجلس التأكد، من خلال لجنة التدقيق المنبثقة عنه، من التزام المُدقِّق الداخلي والمُدقِّق الخارجي للمؤسسة، لدى تنفيذ عمليات التدقيق المختص للمعلومات والتقنية ذات الصلة، بما يأتي:

1- معايير تدقيق تقنية المعلومات والاتصالات بحسب آخر تحديث للمعيار الدولي ( Information Technology Assurance Framework) (ITAF) الصادر عن جمعية التدقيق والرقابة على نظم المعلومات (ISACA) ومنها:
- تنفيذ مهمات التدقيق ضمن خطة معتمدة بهذا الشأن تأخذ بالحسبان الأهمية النسبية للعمليات ومستوى المخاطر ودرجة التأثير في أهداف ومصالح المؤسسة.
- توفير والالتزام بخطط التدريب والتعليم المستمر من قبل الكادر المتخصص بهذا الصدد.
- الالتزام بمعايير الاستقلالية المهنية والإدارية وضمان عدم تضارب المصالح الحالية والمستقبلية.
- الالتزام بمعايير الموضوعية وبذل العناية المهنية والحفاظ المستمر على مستوى التنافسية والمهنية من المعارف والمهارات الواجب التمتع بها، ومعرفة عميقة في آليات وعمليات المؤسسة المختلفة المرتكزة على تقنية المعلومات والاتصالات وتقارير المراجعة والتدقيق الأُخرى (المالية والتشغيلية والقانونية)، والقدرة على تقييم

الدليل المتناسب مع الحالة والوضع العام في كشف الممارسات غير المقبولة والمخالفة لأحكام القوانين والأنظمة والضوابط.

2- فحص عمليات توظيف وإدارة موارد 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 في الأقل المحاور المبينة في المرفق رقم (5) على أن يكون تكرار التدقيق للمحاور كافّةً أو جزء منها، حدًّا أدنى مرة واحدة سنويًّا في الأقل في حال تمّ تقييم المخاطر بدرجة (5 أو4) بحسب سُلّم تقييم المخاطر الموضح في المرفق رقم (4)، ومرّةً واحدة كُلّ سنتين في الأقل في حال تمّ تقييم المخاطر بدرجة (3)، ومرّةً واحدة كُلّ ثلاث سنوات في الأقل في حال تمّ تقييم المخاطر بدرجة (2 أو1)، مع مراعاة التغيُّر المستمر في مستوى المخاطر والأخذ بالحسبان التغيُّرات الجوهرية التي تطرأ على بيئة المعلومات والتقنية ذات الصلة خلال مُدد التدقيق المذكورة، على أن يتمّ تزويدنا بتقارير التدقيق لأوّل مرة بغض النظر عن درجة تقييم المخاطر، وعلى أن تشمل عمليات التقييم للمحاور المذكورة آليات المؤسسة المتبعة، من حيث التخطيط الاستراتيجي ورسم السياسات، والمبادئ وإجراءات العمل المكتوبة والمعتمدة، وآليات توظيف الموارد المختلفة، بما فيها موارد تقنية المعلومات والاتصالات والعنصر البشري، وآليات وأدوات المراقبة والتحسين والتطوير، والعمل على توثيق نتائج التدقيق وتقييمها استنادًا إلى أهمّية الاختلافات ونقط الضعف (الملحوظات)، فضلًا عن الضوابط المفعّلة وتقييم مستوى المخاطر المتبقية والمُتعلِّقة بكل منها باستخدام معيار منهجي لتحليل وقياس المخاطر، متضمّنًا الإجراءات التصحيحية المُتَّفَق عليها، والمَنويّ اتباعها من قبل إدارة المؤسسة بتواريخ مُحدَّدة للتصحيح، مع الإشارة ضمن جدول خاص إلى رتبة صاحب المسؤولية في المؤسسة المسؤول عن ملاحظاته.

3- إجراءات منتظمة لمتابعة نتائج التدقيق للتأكد من معالجة الملحوظات والاختلافات الواردة في تقارير المُدقِّق بالمواعيد المحدَّدة، والعمل على رفع مستوى الأهمية والمخاطر تصعيدًا تدريجيًّا في حال عدم الاستجابة، وإعلام المجلس بذلك كلما تطلّب الأمر.

4- تضمين آليات التقييم السنوي (Performance Evaluation) لكوادر تدقيق تقنية المعلومات والاتصالات بمعايير قياس موضوعية، على أن تتمّ عمليات التقييم من قبل المجلس ممثلًا بلجنة التدقيق المنبثقة عنه، وبحسب التسلسل الإداري التنظيمي لدوائر التدقيق، أو مَن يحلُّ محلها في المصارف الأجنبية.

هـ - من الممكن إسناد مَهمّة المُدقِّق الداخلي للمعلومات والتقنية ذات الصلة (Internal IT Audit) إلى جهة خارجية مختصّة مستقلة تمامًا عن المُدقِّق الخارجي المعتمد بهذا الشأن (Outsourcing)، شريطة تلبية جميع متطلبات هذه الضوابط، وأيّة ضوابط أُخرى ذات صلة، واحتفاظ لجنة التدقيق المنبثقة عن المجلس، والمجلس نفسه بوظيفتهما، فيما يتعلق بفحص الامتثال والتأكد من تلبية هذه المتطلبات، حدًّا أدنى.

**سابعًا: الإطار العام لإدارة مخاطر تقنية المعلومات والاتصالات**

تُشكَّل لجنة لإدارة المخاطر منبثقة عن مجلس إدارة المؤسسة بحسب دليل الحوكمة المؤسسية الصادر عن البنك المركزي مهامها وضع استراتيجية، وإدارة الأدوار والمسؤوليات في عملية إدارة المخاطر، وتوزيعها، إلى جانب وجود قسم إدارة المخاطر في كُلّ مؤسسة يتولى جميع مهام وفعاليات إدارة المخاطر لتقنية المعلومات والاتصالات، وتتشكَّل هذه اللجنة من ثلاثة أعضاء في الأقل من الأعضاء غير التنفيذيين على أن يكون رئيس اللجنة عضو مستقل، ويجب أن يمتلك أعضاء اللجنة الخبرة أو المعرفة في إدراة المخاطر والممارسات 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 أُصول نظام المعلومات.
3. تحديد وتقييم التهديدات والمخاطر المحتملة ونقط الضعف الحالية والناشئة.
4. تطبيق المعايير الدولية (ISO 31000، NIST، COBIT for RISK، ISO/IEC 27005:2018، IT GXM).
5. تطبيق الممارسات والرقابة المناسبة للتخفيف من المخاطر.

6. تحديث دوري وتقييم للمخاطر بما يشمل التغييرات في النظم البيئية أو الظروف التشغيلية التي قد تؤثر في تحليل المخاطر.

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

**حماية أُصول (موجودات) أنظمة تقنية المعلومات والاتصالات**

الحماية الكافية والمناسبة لأُصول النظام من الوصول غير المخول وسوء الاستخدام والاحتيال والإدراج والحذف والاستبدال والكشف والإلغاء، يجب على المؤسسة وضع سياسات واضحة لحماية أُصول النظام وتحديد أهميته والتحقق من صحته من أجل وضع خطط مناسبة لحمايته.

**عملية إدارة المخاطر**

المخاطر هي دالة على احتمال وجود مصادر تهديد مُعيّنة نتيجة نقط ضعف محتملة، يترتب عليها أثر سلبي في المنظمة بشكل عامّ، ولتحديد احتمال وقوع حدث سلبي مستقبلي يجب تحليل التهديدات التي تتعرّض لها نظم تقنية المعلومات، بالاقتران مع نقط الضعف المحتملة والضوابط المعمول بها، إذ تتضمّن عملية إدارة المخاطر البدء بتحليل بيئة الخطر، وتحديد المخاطر، وتحليلها، وتقييمها، ومعالجتها، من خلال عملية مستمرة وفقاً لمعيار ISO:31000 المعتمدة، على النحو المُبيَّن فيما يأتي:

1- **تحليل بيئة تقنية المعلومات**

يتطلب تحديد المخاطر لتقنية المعلومات الفهم الدقيق لبيئة النظم؛ لذلك يجب جمع المعلومات المتعلقة بتقنية المعلومات، والتي عادةً ما تُصنَّف 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 أهميّته للمؤسسة.
حساسية النظام والبيانات، ومستوى الحماية المطلوبة للحفاظ على النظام وسلامة البيانات، والسرية وتوافرها.

2- **تقدير المخاطر**

أ- **تحديد المخاطر**

- **التعرُّف على التهديدات**

يجب تحديد التهديدات وأوجه الضعف في بيئة تقنية 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 يتسبّب في أضرار من خلال استغلال الضعف في النظام. ويمكن أن يكون مصدر التهديد من العوامل الطبيعية أو العوامل البشرية أو العوامل البيئية. وتُعَدُّ العوامل البشرية من أهمّ مصادر التهديدات من خلال الأخطاء المُتعمّدة أو غير المُتعمّدة التي يمكن أن تُلحِق ضرراً شديداً بالمؤسسة، ونظم المعلومات الخاصة بها، عند إدارتها من قبل أشخاص غير أكفاء.

التهديدات الأمنية كتلك التي تتجلّى في هجمات المنع من الخدمة، والتخريب الداخلي، وهجمات البرمجيات الخبيثة، يمكن أن تَتَسبَّب في ضرر شديد، وتعطيل لعمليات المؤسسة، والخسائر اللاحقة لجميع الأطراف المتضررة. ويجب أن تكون المؤسسة يقظة في مراقبة مثل هذا النوع من المخاطر المتغيّرة والمتنامية؛ لأنّها خطوة مهمة في ممارسة احتواء هذه المخاطر.

- **التعرُّف على قابلية التعرُّض للتهديدات**

يجب أن يتضمّن تحليل التهديدات لتقنية المعلومات تحليلاً لنقط الضعف المرتبطة مع بيئة النظام، والهدف هو التعرُّف على (العيوب أو نقاط الضعف) التي يمكن استغلالها من مصادر التهديد المحتملة.

**ب- تقييم المخاطر**

- **تحديد الاحتمالية**

لتحديد احتمالية إمكانية التعرُّض لتهديد محتمل لأنظمة تقنية المعلومات يجب مراعاة العوامل الآتية:

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

ويمكن وصف احتمالية تعرُّض الثغرات المحتملة لمصدر تهديد مُعيّن بأنّها عالية، أو متوسطة، أو منخفضة.

- **تحليل الأثر**

هي عملية تحديد الأثر السلبي الناشئ عن تحقُّق 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 مستوى المخاطر**

تحديد مستوى المخاطر التي تتعرَّض لها نظم تقنية المعلومات، ويمكن التعبير عنه دالةً لـ:

- احتمال وجود مصدر تهديد أو خطر مُعيّن نتيجة نقطة ضعف مُعيّنة.
- مستوى التأثير الناتج عن الثغرات الأمنية، في النظام وممارسة مصدر التهديد بنجاح.
- مدى كفاية الضوابط الأمنية المُخطَّط لها، أو القائمة، لتقليل المخاطر أو القضاء عليها.

**ج- معالجة المخاطر**

- لكل نوع من أنواع المخاطر يجب تنفيذ استراتيجيات التخفيف والرقابة التي تتفق مع أُصول النظام ومستوى تحمُّل المخاطر.
- يستلزم تخفيف المخاطر واتباع أُنموذج منهجي لتقييم وتحديد أولويات الضوابط المناسبة للحدّ من المخاطر. ومن مجموعة من الضوابط الفنية والإجرائية والتشغيلية والوظيفية التي من شأنها توفير طريقة فعّالة لتقليل المخاطر.
- قد لا يكون من العملي معالجة 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 تسبّب ضرراً كبيراً على عمليات المؤسسة. ويجب على المؤسسة تقييم قدرتها على تحمُّل المخاطر والأضرار والخسائر في حالة وقوع حدث مُعيَّن، وينبغي أيضًا أن تكون هناك موازنة بين تكاليف الرقابة على المخاطر وبين الفوائد المتأتية منها.

- من الضروري أن تكون المؤسسة قادرة على إدارة المخاطر ومراقبتها بطريقة تُحافظ بها على سلامة واستقرار الوضع المالي والتشغيلي. وعند تبنّي الرقابة البديلة وتدابير أمنية جديدة يجب على المؤسسة أن تكون مدركةً لتكاليف وفاعلية الرقابة المتعلّقة بالمخاطر التي يتمُّ تخفيفها.
- يجب على المؤسسة عدم تطبيق، أو تشغيل أيّ نظام ضعيف، أو لا يمكن فيه مواجهة مخاطر النظام ومراقبتها بشكل كافٍ.
- بصفة إجراء مُخفّف للمخاطر يمكن للمؤسسة الحصول على بوليصة تأمين لتغطية مختلف المخاطر القابلة للتأمين، بما في ذلك تكاليف الإصلاح والتعويض.

**رصد المخاطر وإعداد التقارير**

- يجب أن تحتفظ المؤسسة بسجل للمخاطر مما يسهل عملية الرقابة على المخاطر والإبلاغ عنها. وينبغي إعطاء الأولوية القصوى للمخاطر الشديدة ورصدها عن كثب، مع الإبلاغ المنتظم عن الإجراءات التي اتخذت للتخفيف منها. كما ينبغي للمؤسسة أن تقوم بتحديث سجلات المخاطر بشكل دوري، وأن تتم عمليات الرقابة والمراجعة لتقييم المخاطر ومعالجتها بشكل مستمر.
- لتسهيل إعداد تقارير المخاطرة للإدارة يجب على المؤسسة تطوير وحدات قياس لمخاطر التقنية بحسب الأنظمة، أو العمليات والبنية التحتية التي لديها أعلى نسب تعرض للمخاطر. كما يجب أيضًا 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 وملحوظات التدقيق.
- قد تتغير عوامل قياس المخاطر مع تغير بيئة تقنية المعلومات والاتصالات وقنوات التوزيع. ومن ثَمَّ يجب على المؤسسة مراجعة وتحديث عمليات إدارة المخاطر وفقًا لذلك وإجراء إعادة تقييم لأساليب مراقبة المخاطر السابقة مع اختبار متجدّد، وتقييم مدى كفاية وفعالية عمليات إدارة المخاطر.
- يجب أن تقوم إدارة التقنية بمراجعة وتحديث نهج التحكُّم في مخاطر تقنية المعلومات والاتصالات والتخفيف منه، مع مراعاة الظروف المتغيّرة والتغيّرات في المخاطر المُتعلِّقة بالمؤسسة.

**الإشراف على مخاطر تقنية المعلومات والاتصالات من قبل مجلس الإدارة والإدارة العليا**

- تُعَدُّ تقنية المعلومات والاتصالات الوظيفة الأساس لكثير 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 فوريًّا 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 تقنية المعلومات والاتصالات في دعم أعمال المؤسسات المصرفية، يجب على مجلس الإدارة والإدارة العليا، الإشراف على مخاطر التقنية والتأكد من أنّ 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 أيضًا أن تتمّ مشاركة القرارات الاستراتيجية والمُهمّة لتقنية المعلومات والاتصالات فيما بينهم.
- يجب على مجلس الإدارة أن يكون مسؤولًا 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 والآثار القانونية، المُتعلِّقة بالاستثمار في عمليات الرقابة وإجراءات الحماية الخاصة لكل من أنظمة الحاسوب والشبكات ومراكز البيانات ("DC") وعمليات وتسهيلات النسخ الاحتياطي.

**2) سياسات تقنية المعلومات والاتصالات والمعايير والإجراءات**

- يجب على المؤسسات المصرفية وضع السياسات والمعايير الخاصة بتقنية المعلومات والاتصالات، والتي تُعَدُّ من المكونات الأساس لإطار إدارة مخاطر التقنية وحماية أُصول النظام في المؤسسة.
- بسبب التغيرات السريعة في عمليات تقنية 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 يتمّ معالجة الانحرافات عن الامتثال ومعالجتها في الوقت المناسب.

**3) عمليات اختيار الأشخاص**

- الاختيار الدقيق للموظفين والمزوّدين والمتعاقدين، أمر بالغ الأهمية؛ لتقليل مخاطر التقنية المتمثلة في فشل النظام والتخريب الداخلي والاحتيال. وبما أنَّ الأشخاص يلعبون دورًا مُهمًّا في إدارة الأنظمة والعمليات المُتعلِّقة ببيئة تقنية المعلومات والاتصالات، فيجب على المؤسسات المصرفية تنفيذ عمليات فحص شاملة وفعالة.
- ينبغي أيضًا أن يُطلَب من الموظفين والمزوّدين والمتعاقدين المخوَّلين بالوصول إلى الأنظمة في المؤسسات المصرفية، حماية المعلومات الحساسة 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 أيضًا أن يتضمن البرنامج التدريبي معلومات عن سياسات ومعايير أمن تقنية المعلومات والاتصالات، فضلًا عن المسؤوليات الفردية والتدابير التي يجب اتخاذها لحماية أُصول النظام. يجب أن يكون كُلّ 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 والحاليين والمتعاقدين والمزوّدين الذين يستطيعون الوصول إلى موارد وأنظمة تقنية المعلومات والاتصالات في المؤسسة.
- ينبغي اعتماد برنامج التدريب من قبل الإدارة العليا. وينبغي مراجعته وتحديثه بإستمرار للتأكد من أنّ محتويات البرنامج مُحدَّثة ومناسبة، وأن تأخذ المراجعة بالحسبان البيئة المتطورة للتقنية، فضلًا عن المخاطر الناشئة.

**إدارة مخاطر الإسناد إلى مصادر خارجية (outsourcing) لتقنية المعلومات والاتصالات**

الإسناد إلى مصادر خارجية (outsourcing) تأتي في كثير من الأشكال. بعض الأنواع الأكثر شيوعًا في الإسناد إلى مصادر خارجية (outsourcing) لتقنية 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 متعدّدين موجودين في العراق أو في الخارج.

**الإجراءات لإرضاء المتطلبات**

- ينبغي على مجلس الإدارة والإدارة العليا فهم المخاطر الكاملة المرتبطة بالإسناد إلى مصادر خارجية (outsourcing) لتقنية المعلومات والاتصالات. قبل تعيين المزوّدين، 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 المتعاقدة بشكل كامل في اتفاقيات خطية، وعادةً ما تشمل المتطلبات والشروط التي تُغطّى في الاتفاقيات،

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

- يجب على المؤسسة التأكد من أنّ مزوّد الخدمات يمنح حق الوصول إلى جميع الأجزاء التي رشحتها المؤسسة للأنظمة والعمليات والوثائق الخاصة بها من أجل إجراء أيّة مراجعة أو تقييم لأغراض التنظيم أو التدقيق أو الامتثال.
- لا ينبغي أن تؤدّي عمليات الإسناد إلى مصادر خارجية (outsourcing)، إلى إضعاف وتدهور الرقابة الداخلية للمؤسسة. يجب على المؤسسة أن يطلب من مزوّد الخدمة توظيف مستوى عالٍ 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 ومزوّد الخدمة الخارجي (External Service Provider) توقيع اتفاقية المحافظة على سرية المعلومات والبيانات NDA(Non-Disclosur Agreement)، فضلًا عن اتفاقية عدم تعيين موظفي المؤسسة لدى مزوّد 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 مزوّد الخدمة تنفيذ السياسات الأمنية وإجراءات الرقابة ويجب أن تكون الإجراءات محكمة كما يطّبقها المزوّد للنشاطات الخاصة به.
- يجب على المؤسسة مراقبة ومراجعة السياسات الأمنية وإجراءات الرقابة لمزوّد الخدمة على أساس منتظم، بما في ذلك الحصول على تقارير دورية عن مدى كفاية نشاطات الحماية، والالتزام فيما يتعلق بالعمليات والخدمات التي يقدّمها مزوّد الخدمة.
- يجب على المؤسسة أن تطلب من مزوّدي الخدمة تطوير وإنشاء إطار للتعافي من الكوارث الطارئة، ويجب أن يتمّ تحديد المهام والمسؤوليات في توثيق وحماية واختبار خطط الطوارئ والتعافي من الكوارث.
- يجب أن تتلقى جميع الأطراف المعنية بما في ذلك مُقدّمي الخدمات، تدريبًا منتظمًا على تفعيل خطة الطوارئ وتنفيذ إجراءات التعافي.
- يجب مراجعة خطة التعافي من الكوارث وتحديثها واختبارها بانتظام وفقًا للظروف المتغيرة والمتطلبات التشغيلية.
- يجب على المؤسسة أيضًا وضع خطة طوارئ تستند إلى أسوء سيناريوهات تعطل الخدمة؛ للتحضير لاحتمال عدم قدرة مزوّدي الخدمة الحاليين على مواصلة العمليات وتقديم الخدمات المطلوبة. ويجب أن تتضمن الخطة تحديد بدائل قابلة للاستمرار لاستئناف عملياتها في مجال تقنية المعلومات والاتصالات في أماكن أخرى.

## الحوسبة السحابية (Cloud Computing)

- الحوسبة السحابية هي أنموذج خدمات ونقل معلومات لتمكين الوصول إلى الشبكة بحسب الطلب لمجموعة مشتركة من موارد الحوسبة القابلة للتكوين (الخوادم والتخزين والخدمات). وقد لا يعرف مستخدمو مثل هذه الخدمات المواقع الدقيقة للخوادم والتطبيقات والبيانات داخل البنية الأساسية للحوسبة لمُقدّم 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 سيّما في مجالات تكامل البيانات، والسيادة، والنزاهة، والاستئجارات المتعدّدة للمنصة، والاسترداد، والسرية، والامتثال التنظيمي، والتدقيق، ونقل البيانات إلى الخارج.
- بما أنّ موردي خدمات الحوسبة السحابية قد يعتمدون الأساليب الممزوجة والإيجارات المتعددة من أجل معالجة بيانات الزبائن، فيجب على المؤسسة الانتباه إلى قدرات مزوّدي الخدمة وتحديد بيانات الزبائن وموجودات النظام بشكل واضح من أجل حمايتها.
- في حالة انتهاء العقد مع مزوّد الخدمة، سواء عند انتهاء الصلاحية أم قبل المدة المحددة، يجب أن تمتلك المؤسسة السلطة التعاقدية والوسائل اللازمة لإزالة البيانات المُخزّنة على الفور في أنظمة مزوّد الخدمة والنسخ الاحتياطية.
- يجب على المؤسسة التحقُّق من قدرة مزوّد الخدمة على تعافي الأنظمة الخارجية، وخدمات تقنية المعلومات والاتصالات، ضمن الهدف الزمني للتعافي المُحدَّد قبل التعاقد مع مزوّد 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) التزودّ 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.

**ثامنًا: ضوابط حوكمة وإدارة المعلومات والتقنية ذات الصلة**

على المؤسسة القيام بتطوير دليل خاص لحوكمة وإدارة المعلومات والتقنية ذات الصلة، وقد يكون جزءًا من دليل الحوكمة المؤسسية، بحيث يأخذ الدليل بالحسبان هذه الضوابط حدًّا أدنى، وبشكل ينسجم واحتياجاته وسياساته، وأن يتمّ اعتماد الدليل من المجلس، وتزويد البنك المركزي به خلال مدّة اقصاها (6 أشهر) من تاريخ هذه الضوابط، وبحيث يُعبّر 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 تقنية المعلومات والاتصالات المنبثقة عن المجلس مراجعة هذا الدليل وتحديثه كلما اقتضت الحاجة.

**المبادئ والسياسات وأطر العمل**

- على المجلس، أو مَنْ يُفوّض 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 تقنية المعلومات والاتصالات، الواردة في المرفقين (2) و(3) على الترتيب.
- على المجلس، أو مَنْ يُفوّض من لجانه، اعتماد المبادئ والسياسات وأُطر العمل، وبصورة خاصة تلك المُتعلّقة بإدارة مخاطر تقنية المعلومات والاتصالات، وإدارة أمن المعلومات، وإدارة الموارد البشرية التي تلبي متطلبات عمليات حوكمة تقنية المعلومات والاتصالات، الواردة في المرفق رقم (3).
- على المجلس، أو مَنْ يُفوّض من لجانه، اعتماد منظومة السياسات اللازمة لإدارة موارد وعمليات حوكمة تقنية المعلومات والاتصالات، الواردة في المرفق رقم (6)، وعدّ منظومة السياسات هذه حدًا أدنى، مع إمكانية الجمع والدمج لتلك السياسات بحسب ما تقتضيه طبيعة العمل، على أن يتمّ تطوير سياسات أُخرى ناظمة مواكبة لتطور أهداف المؤسسة وآليات العمل، وعلى أن تحدد كُلّ سياسة الجهة المالكة، ونطاق التطبيق، ودورية المراجعة والتحديث، وصلاحيات الاطلاع، والتوزيع، والأهداف، والمسؤوليات وإجراءات العمل المُتعلّقة بها، والعقوبات في حال عدم الامتثال، وآليات فحص الامتثال.
- يُراعى لدى إنشاء السياسات مساهمة جميع الشركاء الداخليين والخارجيين واعتماد أفضل الممارسات الدولية وتحديثاتها بوصفها مراجع لصياغة تلك السياسات مثل ( COBIT, ISO/IEC 27001/2,ISO 31000, ISO/IEC 9126, ISO/IEC 15504, ISO 22301, PCI DSS, ITIL,...etc).

**الهياكل التنظيمية**

- على المجلس اعتماد الهياكل التنظيمية (الهرمية واللجان) وبصورة خاصة تلك المُتعلّقة بإدارة موارد وعمليات ومشاريع تقنية المعلومات والاتصالات، وإدارة امن المعلومات، وإدارة الموارد البشرية التي تلبي متطلبات عمليات حوكمة تقنية المعلومات والاتصالات وتحقيق أهداف المؤسسة بكفاءة عالية وفعالية.

- يُراعَى ضمان فصل المهام المتعارضة بطبيعتها ومتطلبات الحماية التنظيمية المُتعلِّقة بالرقابة الثنائية حدًّا 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 مرتكزًا 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، فضلًا 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 المقيّد ( objectivity, believability, Reputation, Relevancy, Appropriate Amount, Concise Representation, Consistent Representation, Interpretability, understandability, Ease of manipulation, Restricted Access)

- على المجلس أو مَنْ يُفوِّض من لجانه اعتماد منظومة المعلومات والتقارير الواردة في المرفق رقم (7)، وعدّ تلك المنظومة حدًّا أدنى مع مراعاة تحديد مالكين لتلك المعلومات والتقارير تُحدَّد من خلالهم، وتُفوّض صلاحيات الاطلاع والاستخدام بحسب الحاجة للعمل والشركاء المعنيين، على أن تتمّ مراجعتها وتطويرها بشكل مستمر لمواكبة تطوير أهداف وعمليات المؤسسة وبما يوافق أفضل الممارسات الدولية المقبولة بهذا الشأن.

**الخدمات والبرامج والبنية التحتية لتقنية المعلومات والاتصالات:**

- على المجلس أو مَنْ يُفوِّض من لجانه والإدارة التنفيذية العليا اعتماد منظومة الخدمات والبرامج والبنية التحتية لتقنية المعلومات والاتصالات، الواردة في المرفق رقم (8)، وعدّ تلك المنظومة حدًّا أدنى، على أن يتمّ توفيرها وتطويرها بشكل مستمر لمواكبة تطور أهداف المؤسسة وعملياتها، وبما يوافق أفضل الممارسات الدولية المقبولة بهذا الشأن.

- على المجلس أو مَنْ يُفوِّض من لجانه والإدارة التنفيذية العليا اعتماد منظومة الخدمات والبرامج والبنية التحتية لتقنية المعلومات والاتصالات الداعمة والمساعدة لتحقيق عمليات حوكمة تقنية المعلومات والاتصالات، ومن ثَمَّ أهداف المعلومات والتقنية المصاحبة لها، والأهداف المؤسسية.

**المعارف والمهارات والخبرات:**

- على المجلس أو مَنْ يُفوِّض من لجانه اعتماد مصفوفة المؤهلات (HC Competences) وسياسات إدارة الموارد البشرية اللازمة لتحقيق متطلبات عمليات حوكمة تقنية 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 استنادًا إلى معايير الخبرات الأكاديمية والفنية والمهنيّة من خلال تأشيرها من جهات ذات اختصاص، على أن تتمّ إعادة تأهيل وتدريب الكوادر الموظفة حاليًا 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 تقنية المعلومات والاتصالات، الواردة في المرفق رقم (3).

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

**تاسعًا: اقتناء وتطوير نظم المعلومات والاتصالات**

- قد تفشل كثير من الأنظمة بسبب ضعف في تصميم وتنفيذ النظام، فضلًا 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 تقدُّم المشروع، بما في ذلك الأهداف التي يجب تحقيقها في كُلّ مرحلة من مراحل المشروع والأحداث المهمّة التي سيتم الوصول إليها وفقًا للجدول الزمني للمشروع وخطة تنفيذ المشروع (Project Plan)، وللمؤسسة تحديد الهيكلية الهرمية لتنفيذ كُلّ مشروع.

**إدارة التغيير وتوثيق عملية التغيير**

- يجب أن تنشئ المؤسسة عملية إدارة التغيير لضمان تقييم التغييرات في أنظمة الإنتاج والموافقة عليها وتنفيذها ومراجعتها بطريقة خاضعة للرقابة.
- يجب تطبيق عملية إدارة التغيير على التغييرات المُتعلِّقة بالنظام، ومكوّنات 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 أيضًا تحديد ما إذا كان التغيير الذي تمّ إدخاله سيؤدي إلى حدوث مشاكل أمنية أو مشاكل في توافق البرامج مع الأنظمة أو التطبيقات المتأثرة.
- يجب على المؤسسة اختبار التغيرات الوشيكة بشكل كافٍ وضمان قبوله من قبل المستخدمين قبل نقل النماذج التي تمّ تغييرها إلى نظام الإنتاج. ويجب أيضًا 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 أيضًا 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 يتمّ تنفيذها أثناء عملية الترحيل.

**متطلبات الحماية والإختبارات**

- يجب أن تُحدِّد المؤسسة بوضوح متطلبات الحماية المُتعلِّقة في الوصول إلى النظام، والتوثيق، وترخيص المعاملات، وسلامة البيانات، وتسجيل نشاط النظام، ومراجعة الحسابات، وتتبُّع الأحداث الأمنية، ومعالجة الاستثناءات في المراحل المبكرة من تطوير النظام أو اقتنائه. ويجب على المؤسسة أيضًا 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 أيضًا إجراء فحص الضعف لمكوّنات الشبكة الخارجية والداخلية التي تدعم النظام الجديد.

- يجب أن تحتفظ المؤسسة ببيئات منطقية أو مادية منفصلة للوحدات والتكامل، فضلًا عن النظام واختبار قبول المستخدم (User Acceptance Testing "UAT") وأن تراقب عن كثب وصول المزوّدين والمطوّرين إلى بيئة اختبار قبول المستخدم ("UAT").

**مراجعة رموز المصدر**

- هناك طرائق مختلفة لبرامج التشفير التي قد تخفي التهديدات الأمنية والثغرات سواء كانت متعمدة أم غير متعمدة. عادةً ما تكون اختبارات قبول النظام والمستخدم غير فعّالة في اكتشاف الرموز الضارة، فايروسات، فإنّ اختبار الصندوق الأسود ليس أداة فعّالة في تحديد أو كشف هذه التهديدات الأمنية ونقط الضعف.
- مراجعة رموز المصدر هي فحص منهجي لرمز المصدر للتطبيقات بهدف إيجاد عيوب ناجمة عن أخطاء في التشفير أو ممارسات ترميز ضعيفة أو هجمات خبيثة. وهي مُصمّمة لتحديد مواطن الضعف وأوجه القصور الأمنية والأخطاء في تصميم النظام أو وظائفه المُتعلّقة 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 كافّةً. ويجب أن تمارس المؤسسة الإجراءات لإرضاء المتطلبات للتأكد من أن تطبيقاتها لديها نظام رقابة مناسب، مع مراعاة نوع وتعقيد الخدمة التي تُقدّمها هذه التطبيقات.
- بناءً على تحليل المخاطر في المؤسسة يجب أن يختبر النظام بشكل صارم وحدات تطبيق مُحدّدة إجراءات أمنية مع مجموعة من مراجعة رموز المصدر واختبار الاستثناء ومراجعة الامتثال لتحديد ممارسات الترميز الخاطئة ونقط ضعف الأنظمة التي قد تؤدي إلى حدوث مشاكل أمنية 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.

**عاشرًا: إدارة مشاريع تقنية المعلومات والاتصالات**

- عند إعداد الإطار العام لإدارة المشروع، يجب على المؤسسة التأكد من أنّ 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 أيضًا أن تُحدّد 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 تُحدّد بوضوح المخرجات التي يجب تحقيقها في كُلّ مرحلة من مراحل المشروع، فضلًا 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، يتمّ 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؛ لتجنّب الأخطاء، وعدم التراجع والعودة إلى الإصدار السابق.

**الحادي عشر:إدارة خدمات تقنية المعلومات والاتصالات**

يُعَدُّ الإطار لإدارة خدمة تقنية المعلومات والاتصالات ضروريًا لدعم أنظمة تقنية المعلومات والاتصالات وخدماتها وعملياتها وإدارة التغييرات والمشكلات، فضلًا 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، فضلًا عن إدارة القدرات.

**ترحيل البرامج**

- يتضمن ترحيل البرامج نقل الرموز والبرامج النصية من بيئة البرمجة إلى بيئات الاختبار والإنتاج. ويمكن أن تتسبب الرموز غير المُصرَّح بها أو الضارة التي يتمّ حقنها أثناء عملية الترحيل، في تعرُّض 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 يتمّ تنفيذ التغيير بنجاح في بيئة الإنتاج، يجب أيضًا أن يتمّ تكرار التغيير وترحيله إلى أنظمة التعافي من الكوارث أو تطبيقات لعمليات التوافق.

**إدارة الحوادث**

- يجب على المؤسسة إنشاء إطار لإدارة الحوادث بهدف استعادة خدمات تقنية المعلومات والاتصالات بشكل طبيعي بأسرع ما يمكن بعد وقوع الحادث، مع الحد الأدنى من التأثير في عمليات المؤسسة، ويجب أيضًا تحديد مهام ومسؤوليات الموظفين المشاركين في عملية إدارة الحوادث، التي تشمل تسجيل الحوادث وتحليلها ومعالجتها ورصدها.
- تحصل الحوادث في تقنية المعلومات والاتصالات عندما يكون هناك خلل غير متوقع في موعد التسليم القياسي لخدمات تقنية المعلومات والاتصالات، ويجب على المؤسسة إدارة مثل هذه الحوادث بشكل مناسب لتفادي أيّة حالات سوء معالجة تؤدي إلى تعطيل طويل الأمد لخدمات تقنية المعلومات والاتصالات أو مزيد من التفاقم.
- من المهم أن تتلاءم معالجة الحوادث بحسب مستوى الخطورة المناسب. بوصفه جزءًا من تحليل الحوادث، ويجوز للمؤسسة أيضًا انتداب 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. فضلًا عن ذلك يجب تحديد وتوثيق المعايير المستخدمة لتقييم 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 مسبقًا للحوادث الأمنية على أساس منتظم.
- يجب تشكيل فريق استجابة طوارئ للحواسيب، يضم موظفين داخل المؤسسة مع المهارات الفنية والتشغيلية اللازمة للتعامل مع 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 التعافي من الكوارث في الوقت المناسب، ويجب أن تقوم المؤسسات المصرفية بإبلاغ البنك المركزي بأسرع وقت ممكن في حالة فشل النظام في استعادة القدرة على العمل بعد الكوارث وأن يتمّ إنشاء إجراءات لإبلاغ البنك المركزي العراقي 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 بأيّة حوادث مهمة قد تحصل. ويجب تقييم فعالية طرائق الاتصال، بما في ذلك إعلام الجمهور، عند الضرورة.
- وبما أنّ 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، فضلًا عن ملخص تنفيذي للحدث، وتحليلًا للأسباب الجذرية وتأثيرات الحوادث، فضلًا عن التدابير المتخذة لمعالجة الأسباب الجذرية للحدث الذي يجب أن يغطي ما يأتي:

أ- تحليل السبب الجذري
- متى حدث ذلك؟
- أين حدث؟
- لماذا وكيف وقع الحادث؟
- كم مرة وقعت حادثة مماثلة خلال السنوات الثلاث الماضية؟
- ما هي الدروس المستفادة من هذا الحادث؟

ب- تحليل التأثيرات
- مدى تأثير الحادث ومدته ونطاقه بما في ذلك المعلومات المُتعلّقة 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 نتيجةً للحادث.

ج- التدابير التصحيحية والوقائية

- يجب اتخاذ 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 كافٍ ضمن الإطار الزمني للحلول المتماثلة ومراقبة جميع الحوادث لحلها.

**إدارة المشكلة**

- في حين أنّ الهدف من إدارة الحوادث هو استعادة خدمة تقنية المعلومات والاتصالات في أقرب وقت ممكن، فإنّ الهدف من إدارة المشاكل هو تحديد السبب الجذري للمشكلة والقضاء عليه لمنع حدوث مثل هذه المشاكل المتكررة.
- يجب أن تُحدِّد المؤسسة المهام والمسؤوليات بشكل واضح للموظفين المشاركين في عملية إدارة المشكلات. وتحديد وتصنيف وإعطاء الأولويات ومعالجة جميع المشاكل في الوقت المناسب.
- يجب أن تُحدِّد 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، فضلًا 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 تنشئ المؤسسة عمليات مراقبة واحتساب النسب والحد الأدنى والأعلى لتوفير الوقت الكافي للمؤسسة من أجل عمليات التخطيط وتحديد الموارد الإضافية لتلبية المتطلبات التشغيلية والتجارية بفعالية.

**الثاني عشر: موثوقية الأنظمة وتوافرها واسترجاعها**

- تُعدُّ 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 الحساسة، عادةً ما يكون الأثر في عمليات المؤسسة أو الموظفين شديدًا وواسع الانتشار، وقد تتعرض المؤسسة لعواقب وخيمة على سمعتها جَرَّاء ذلك.
- يجب على المؤسسة تحديد أولويات الاسترداد واستئناف الأعمال واختبار وممارسة إجراءات الطوارئ حتى يتمّ تقليل المشكلات الناشئة عن الحوادث الخطيرة.

**توافرية النظام**

- وتتمثّل العوامل الرئيسة المرتبطة بالحفاظ على توافر النظام بشكل مرتفع في القدرات الكافية والأداء ذي مصداقية ووقت الاستجابة السريع وقابلية التوسع والقدرة على التعافي السريع.
- يجوز للمؤسسة توظيف عدد من مكونات الأنظمة والشبكات المعقّدة 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 عالٍ من التوافرية للأنظمة الحسّاسة.

**خطة التعافي من الكوارث**

- عند صياغة خطة التعافي السريع وبنائها، يجب أن تقوم المؤسسة بتحليل للسيناريوهات ومعالجة مختلف 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 كُلّ 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 الحساسة في رسم خطة التعافي وإجراء اختبارات الطوارئ.
- يجب على المؤسسة تحديد أولويات تعافي النظام، واستئناف الأعمال، ووضع أهداف استرداد مُحدّدة، 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 جغرافيًا 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 مزوّدي خدمة الشبكة المختلفة ومسارات الشبكة البديلة التي يتمّ تأسيسها.

**اختبارات التعافي من الكوارث**

- أثناء انقطاع الخدمة عن النظام، يجب على المؤسسة الامتناع عن اعتماد تدابير التعافي غير المجدية وغير المُجرّبة على إجراءات التعافي المُحدَّدة مسبقًا، والتي تمّ التدرب عليها والموافقة عليها من قبل الإدارة. وتنطوي تدابير التعافي المخصصة على مخاطر تشغيلية عالية إذ لم يتمّ التحقق من فعاليتها من خلال الاختبارات الصارمة والتحقق من صحتها.
- يجب على المؤسسة الاختبار والتحقق في الأقل سنويًا 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، فضلًا عن فشل مكونات النظام الفردي أوعلى مستوى المجموعات، في اختبارات التعافي بعد الكوارث
- يجب على المؤسسة اختبار عمليات التعافي من خلال اعتماد الأنظمة المختلفة. وينبغي إجراء اختبار التعافي الثنائي أو المتعدّد الأطراف إذ ترتبط الشبكات والأنظمة بمُقدِّمي خدمات ومزوِّدين محدّدين.
- يجب على المؤسسة إشراك مستخدمي الأعمال في تصميم وتنفيذ حالات اختبار شاملة للتحقق من أنّ الأنظمة المتعافية تعمل بشكل صحيح. وإشراكهم في اختبارات التعافي بعد الكوارث التي يجريها مُقدِّمو 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 مُحدَّدة، مثل أنظمة التخزين المتصلة المباشرة (DAS)، أو أنظمة التخزين المتصلة بالشبكة (NAS)، أو أنظمة التخزين المحلية الفرعية المتصلة بخوادم الإنتاج (SAN).
- يجب على المؤسسة إجراء اختبارات دورية واختبارات التحقق من استرداد النسخ الاحتياطية وتقييم ما إذا كانت وسائط النسخ الاحتياطي كافية وفعّالة بما فيه الكفاية لدعم عمليات التعافي في المؤسسة.
- يجب على المؤسسة تشفير الأشرطة والأقراص الخاصة بالنسخ الاحتياطية، بما في ذلك وحدات الخزن المتنقلة USB، التي تحتوي على معلومات حسّاسة وسرية قبل نقلها خارج الموقع للتخزين.

**الثالث عشر: إدارة أمن البنية التحتية التشغيلية**

- إنّ نظام تقنية المعلومات والاتصالات عرضة لأشكال مختلفة من الهجمات الإلكترونية، وتزايد وتكرار الهجمات الخبيثة؛ لذا من الضروري أن تقوم المؤسسات المصرفية بتنفيذ حلول أمنية في البيانات والتطبيقات وقواعد البيانات وأنظمة التشغيل وطبقات الشبكة لمعالجة هذه التهديدات واحتواؤها بشكل ملائم.
- ويجب تنفيذ التدابير المناسبة لحماية المعلومات الحساسة والسرية مثل بيانات العميل الشخصية والحسابات والمعاملات التي يتمّ تخزينها ومعالجتها في الأنظمة، ويجب أيضًا أن تتمّ عملية التصديق على الزبائن بشكل صحيح قبل الوصول إلى المعاملات من خلال الإنترنت والمعلومات شخصية ومعلومات الحسابات الحساسة. ويجب تأمين معلومات الزبائن الحسّاسة بما في ذلك بيانات اعتماد تسجيل الدخول، وكلمات المرور، وأرقام التعريف الشخصية (PINs)، ضد عمليات الاستغلال مثل: احتيال البطاقات الائتمانية، واستنساخ البطاقات، والقرصنة، والتصيُّد، والبرامج الضارة.

**منع فقدان البيانات:**

- ومن المحتمل أن يكون التخريب الداخلي أو التجسُّس السري أو الهجمات العنيفة التي يقوم بها الموظفون والمتعاقدون والمزوِّدون الموثوق بهم من بين أخطر المخاطر التي يمكن أن تواجهها المؤسسات المصرفية في بيئة تقنية معلومات ديناميكية ومعقّدة بشكل متزايد، يتميّز الموظفون الحاليون والسابقون والمتعاقدون والمزوِّدون وأولئك الذين لديهم معرفة بالأعمال الداخلية لأنظمة المؤسسة، والعمليات، والرقابة الداخلية على المهاجمين الخارجيين. ولا يُعرّض الهجوم الناجح ثقة الزبائن في أنظمة وعمليات الرقابة الداخلية للمؤسسة فحسب، بل يتسبب أيضًا في خسارة مالية حقيقية عندما يتمّ الكشف عن الأسرار التجارية والمعلومات الخاصة بالمؤسسة. يجب أن تُحدِّد المؤسسة البيانات المهمة وأن تعتمد تدابير مناسبة لاكتشاف ومنع الوصول غير المُخوَّل، أو النسخ، أو نقل المعلومات السرية.
- يجب على المؤسسة تطوير استراتيجية شاملة لمنع فقدان البيانات لحماية المعلومات الحسّاسة والسرية، مع مراعاة النقط الآتية:-

1. البيانات عند نقطة النهاية: البيانات الموجودة في أجهزة الكمبيوتر المحمولة وأجهزة الكمبيوتر الشخصية وأجهزة التخزين المحمولة والأجهزة المحمولة.
2. البيانات قيد الحركة: البيانات التي تمر عبر الشبكة أو يتمّ نقلها بين المواقع.
3. البيانات الأخرى: البيانات في الحواسيب المُخزّنة التي تشمل الملفات المُخزَّنة على الخوادم وقواعد البيانات ووسائل الإعلام الاحتياطية ومنصات التخزين.

- لتحقيق أمن البيانات في نقط النهاية، ينبغي للمؤسسة تنفيذ التدابير المناسبة لمعالجة مخاطر سرقة البيانات وفقدان البيانات وتسربها من أجهزة نقطة النهاية ومواقع خدمة الزبائن ومراكز الاتصال وحماية المعلومات السرية المُخزَّنة في جميع أنواع أجهزة نقط النهاية مع التشفير المتين.
- يجب ألّا تستخدم المؤسسة خدمات الإنترنت غير الآمنة 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 الحسّاسة ، واتخاذ التدابير المناسبة في جميع الأوقات بما في ذلك إرسال المعلومات من خلال القنوات المشفّرة (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 المتسلّمين المستهدفين. بدلاً من ذلك قد تختار المؤسسة وسائل آمنة أخرى لتبادل المعلومات السرية مع المستلمين المستهدفين.
- يجب تشفير وحماية المعلومات السرية المُخزَّنة على أنظمة التقنية والخوادم وقواعد البيانات من خلال ضوابط قوية للوصول، مع الأخذ بالحسبان مبدأ "الأقل امتيازًا".
- 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 تقنية المعلومات والاتصالات**

- لتسهيل تتبّع موارد تقنية المعلومات والاتصالات، يجب على المؤسسة الاحتفاظ بقائمة مُحدَّثة من مكوّنات البرامج والأجهزة المستخدمة في بيئات الإنتاج والتعافي من الكوارث، والتي تشمل جميع الضمانات المرتبطة بها وعقود الدعم الأخرى ذات الصلة بمكوّنات البرامج والأجهزة.
- يجب على المؤسسة إدارة نظم تقنية المعلومات والاتصالات وبرامجها بشكل فعّال، بحيث يتمّ استبدال الأنظمة القديمة وغير المدعومة التي تزيد احتمالية تعرّضها للمخاطر الأمنية في الوقت المناسب. ويجب على المؤسسة أيضًا أن تولي تاريخ انتهاء دعم المنتج ("EOS") عنايةً فائقةً، إذ إنّ من الشائع أن يتوقّف المزوِّدون عن تقديم التصحيحات، بما في ذلك تلك المُتعلِّقة بمواطن الثغرات التي يتمّ 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 المنتج ("EOS") لتقييم مخاطر استمرارية الاستخدام وإنشاء ضوابط فعّالة 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 تُجري المؤسسة فحوصات منتظمة للتأكد من أنّ المعايير الأساسية تُطبَّق بشكل موحد، ويتمّ الكشف عن حالات عدم الامتثال ورفعها للتحقيق. إنّ 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 فإنّ عليها أن تكون على دراية بالمخاطر المرتبطة بهذه البيئة. ويجب تنفيذ جملة من الإجراءات الوقائية من الاختراق مثل بروتوكولات الاتصال الآمنة بين نقط الوصول والزبائن المتصلين لاسلكيًا، لتأمين الشبكة من الوصول غير المُصرَّح 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 واختبارات 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 اليدوية 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 تمّ تحديدها في تقييم الضعف (VA)، ويجري التحقُّق من الصحة بعد ذلك للتحقيق على أنّ الفجوات تتمُّ معالجتها بالكامل.
- يجب على المؤسسة إجراء اختبارات الاختراق من أجل إجراء تقييم متعمّق 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 يتمّ تنفيذها بشكل مناسب يمكن أن يؤثّر ذلك على الأنظمة الفرعية الأخرى. ويجب على المؤسسة أيضًا إجراء اختبار صارم لعمليات التصحيح قبل النشر في بيئة الإنتاج.

**المراقبة الأمنية**

- المراقبة الأمنية هي وظيفة مهمة في بيئة تقنية المعلومات والاتصالات للكشف عن الهجمات الضارة على أنظمة تقنية المعلومات والاتصالات، ولتسهيل الكشف الفوري عن النشاطات غير المُصرَّح 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 أيّ تدخل.
- يجب على المؤسسة استخدام أدوات مراقبة تمكّن من اكتشاف التغييرات في موارد التقنية الأساسية مثل قواعد البيانات أو ملفات النظام أو البيانات، لتسهيل التعرّف على التغييرات غير المُصرَّح 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**

- نظرًا إلى أنّ الأنظمة والبيانات حساسة ومركّزة ومحفوظة في مراكز البيانات، فمن المهم أن تكون مراكز البيانات مرنة ومحمية ماديًا من التهديدات الداخلية والخارجية.

**تقييم مخاطر التهديد والحسّاسية**

- إنّ 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 المُتعلِّقة بمراكز البيانات بناءً على عدد من العوامل، مثل أهمية مراكز البيانات والموقع الجغرافي والاستئجارات المتعددة ونوع المستأجرين الذين يَشغلون 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 المُصرَّح به، والهجمات الخارجية، والتخريب من الداخل.
- يجب على المؤسسة أن تضمن في نطاق تقييم مخاطر التهديد والضعف ("TVRA") مراجعة محيط مراكز البيانات والبيئة المحيطة، فضلًا عن المبنى ومرافق مراكز البيانات ومراجعة الإجراءات الأمنية اليومية، والنظم الميكانيكية والهندسية الحساسة، والبناء والعناصر الهيكلية وكذلك ضوابط الوصول المادية والتشغيلية والمنطقية.
- عند اختيار مزوّدي مراكز البيانات، يجب على المؤسسة الحصول على تقرير تقييم مخاطر التهديد والضعف ("TVRA") وتقييمه على مرافق مركز البيانات. يجب أن تتحقق المؤسسة من أنّ تقارير تقييم مخاطر التهديد والضعف ("TVRA") محدّثة، وأن مزوّدي مراكز البيانات ملتزمون بمعالجة جميع نقط الضعف المادية المحدّدة.

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 المُخوَّلين فقط، وأن يتمّ منح الوصول إلى مراكز البيانات بناءً على الحاجة إليها، ويجب أيضًا إلغاء وصول الموظفين إلى مراكز البيانات فورًا إذا لم تعُدْ هناك حاجة إليهم.
- فيما يخص الموظفين غير المرتبطين بمراكز البيانات مثل المزوّدين 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 أنّ الزوار يُرافقون في جميع الأوقات من قبل موظف معتمد من مراكز البيانات.
- يجب ضمان أنّ المحيط الخارجي لمراكز البيانات والمباني وغرفة المُعدّات تمّ تأمينها ومراقبتها ماديًّا. 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 المُصرَّح به إلى الأنظمة ورفوف المُعدّات والأشرطة.

**مرونة مركز البيانات**

- لتحقيق مرونة في مراكزالبيانات يجب عدم التغاضي عن بعض الأخطاء في مجالات محدّدة مثل الطاقة الكهربائية وتكييف الهواء وأدوات إخماد الحريق واتصالات البيانات.
- يجب على المؤسسة فرض الرقابة على البيئة بشكل منتظم وصارم داخل مراكز البيانات. تُعدُّ مراقبة الظروف البيئية، مثل درجة الحرارة والرطوبة داخل مراكز البيانات أمرًا بالغ الأهمية لضمان وقت التشغيل وموثوقية النظام وتصعيد أيّ خلل يتمّ اكتشافه إلى الإدارة وحلّ المشكلة في الوقت المناسب.
- يجب تنفيذ أنظمة الحماية والإخماد الآلي للحرائق في مراكز البيانات للسيطرة على الحرائق كاملةً في حالة نشوبها، ويجب أيضًا 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 متقطعة وأنظمة البطاريات ومولدات الديزل.
- اعتماد المعايير والمواصفات القياسية العالمية لمراكز البيانات **(DATA CENTER)**. الواردة في المرفق رقم (8).

**الخامس عشر: الرقابة على الوصول للموارد**

هناك ثلاثة من أهم مبادئ الحماية للأنظمة الداخلية وهي:

- . مبدأ عدم العمل المنفرد - بعض وظائف الأنظمة وإجراءاتها ذات طبيعة حساسة 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 - يُعَدُّ الفصل بين المهام عنصرًا أساسيًّا في الرقابة الداخلية. يجب أن تضمن المؤسسة أنّ المسؤوليات والواجبات الخاصة بأنظمة التشغيل وتصميم وتطوير الأنظمة وبرامج صيانة التطبيقات وإدارة الرقابة على الوصول للموارد وأمن البيانات وأمناء وملفات النسخ الاحتياطية يتمّ فصلها وتنفيذها من قبل مجموعات مختلفة من الموظفين. وأنّه يجب أن يتمّ تنظيم تناوب الوظائف وعمليات التدريب لوظائف الإدارة الأمنية. ويجب على المؤسسة تصميم عمليات المعاملات بحيث لا يجوز لأيّ 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 أنّه لا يجوز لأيّ شخص بحكم رتبته أو منصبه

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

**إدارة وصول المستخدمين**

- يجب على المؤسسة منح الوصول إلى الأنظمة والشبكات فقط على أساس الحاجة إلى الاستخدام وخلال المدّة التي يكون فيها الوصول مطلوبًا والتأكد من إعطاء أصحاب الموارد الإذن والموافقة على جميع طلبات الوصول إلى الموارد.
- إن المزوّدين ومُقدّمي الخدمات الذين يمتلكون صلاحيات التخويل بالوصول إلى أنظمة المؤسسة الحساسة وموارد الحواسيب الأخرى، يُشكّلون مخاطر مماثلة مثل المخاطر المُتعلّقة بالموظفين الداخليين للمؤسسة. يجب أن تُخضع المؤسسة الموظفين الخارجيين لعمليات اللإشراف والرقابة وقيود الوصول المماثلة لتلك التي يتمّ تنفيذها للموظفين.
- للمساءلة وتحديد الوصول غيرالمخول، يجب التأكد من أنّ سجلات وصول المستخدم تمّ تحديدها بشكل منفرد وتسجيلها لأغراض التدقيق والمراجعة.
- يجب على المؤسسة إجراء مراجعات منتظمة لامتيازات الوصول للمستخدم للتحقق من منح الامتيازات بشكل مناسب بحسب مبدأ "الأقل امتيازًا". قد تسهل العملية تحديد الحسابات الساكنة والزائدة عن الحاجة، فضلًا عن الكشف عن الوصول الخاطئ.
- تُمثّل كلمات المرور خط الحماية الأوّل وإذا لم يتمّ تنفيذها بشكل مناسب فيمكن أن تكون الحلقة الأضعف في المؤسسة. ومن ثمّ 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، فضلًا عن مدّة الصلاحية وكذلك تحديد الأوقات في اليوم التي يكون خلالها الدخول مسموحًا.
- يجب أن تتأكد المؤسسة من عدم الوصول لأي شخص إلى كُلّ من أنظمة الإنتاج وأنظمة النسخ بشكل متزامن، ولا سيّما ملفات البيانات ومرافق الحواسيب. وأنّ أيّ شخص يحتاج إلى الوصول إلى ملفات النسخ الاحتياطي أو موارد استرداد النظام يجب أن يكون مخوّلًا بحسب الأُصول، وأن تمنح المؤسسة الوصول فقط لأغراض مُحدّدة ولمدّة مُحدّدة.
- يجب على المؤسسة متابعة آخر المستجدات التقنية في مجال التعرف على المستخدمين ومنحهم صلاحيات الوصول والعمل على إدخالها بصفى أساليب بديلة عن كلمات المرور، ومنها تقنيات بصمة الأصبع وبصمة العين.

**إداراة وصول الامتيازات**

- يعتمد أمن المعلومات، في نهاية المطاف، الثقة بمجموعة صغيرة من الموظفين المهرة الذين يجب أن يخضعوا لضوابط ورقابة مناسبة، 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 المُخوّل واكتشاف كلمات المرور وتخريبها، ومسؤولي النظام وموظفي أمن تقنية المعلومات والاتصالات والمبرمجين الذين يقومون بعمليات حرجة ويمتلكون القدرة على إلحاق ضرر شديد بالنظم الحساسة التي يحتفظون بها أو يعملون بحكم وظائفهم المميزة والقدرة على الوصول إلى الامتيازات.
- ينبغي أن تُشرف المؤسسة عن كثب على الموظفين الذين لديهم صلاحيات تخويل مرتفعة للوصول إلى النظام وأن يتمّ تسجيل جميع نشاطاتهم ومراجعتها؛ لأنّ لديهم المعرفة والموارد اللازمة التي قد تُستخدَم أو تسهّل التحايل على أنظمة الرقابة والإجراءات الأمنية، ومن خلال تطبيق إجرءات الرقابة والممارسات الأمنية الآتية:
  - تنفيذ آليات 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 يتمّ فيها التقاط نشاطاته.
- مراجعة نشاطات المستخدمين ذوي الامتيازات في الوقت المناسب.
- حظر مشاركة حسابات الامتيازات.
- منع المزوّدين والمتعاقدين من الحصول على امتيازات الوصول إلى الأنظمة من دون عمليات الإشراف والرقابة عن كثب.
- حماية بيانات النسخ الاحتياطية من الوصول غير المُصرَّح به.

**السادس عشر: الخدمات المالية عبر الإنترنت**

- في حين يُقدِّم الإنترنت فرصًا للمؤسسة للوصول إلى أسواق جديدة وتوسيع نطاق منتجاتها وخدماتها، لكونه شبكة مفتوحة، فإنّه يجلب أيضًا مخاطر أمنية أكثر تطورًا 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 المُقدَّمة عبر الإنترنت. عادةً يمكن تصنيف الخدمات المالية المُقدَّمة عبر الإنترنت إلى خدمات المعلومات وخدمة تبادل المعلومات التفاعلية وخدمة المعاملات. وترتبط مستويات المخاطر المرتفعة مع خدمة المعاملات؛ لأنَّ المعاملات عبر الإنترنت عادةً ما تكون غير قابلة للإلغاء بمجرد أن يتمّ تنفيذها.
- يجب أن تُحدِّد المؤسسة بوضوح المخاطر المرتبطة بأنواع الخدمات المُقدَّمة في عملية إدارة المخاطر. ويجب على المؤسسة أيضًا وضع ضوابط أمنية، وعمليات توافرية النظام، وقدرات عمليات التعافي، التي تتناسب مع مستوى التعرُّض للمخاطر، لجميع عمليات الإنترنت.

**حماية الأنظمة المرتبطة بالإنترنت**

- قد تستهدف الهجمات أنظمة المؤسسة المرتبطة بالإنترنت، إذ يتمّ تقديم الخدمات المالية بشكل متزايد عبر الإنترنت وزيادة الزبائن والمتعاملين، وفي إجراء مضاد، يجب على المؤسسة وضع استراتيجية أمنية، ووضع إجراءات لضمان سرية البيانات والأنظمة وتكاملها وتوافرها.
- يجب تزويد الزبائن والمستخدمين لخدمات الإنترنت بالتأكيدات بأنّ الوصول إلى الإنترنت والمعاملات التي تتمّ عبر الإنترنت على موقع المؤسسة الإلكتروني محمية وموثوقة بشكل كافٍ.
- يجب أن تقوم المؤسسات بتقييم المتطلبات الأمنية المرتبطة بأنظمة الإنترنت بشكل صحيح وتبني خوارزميات التشفير المُعدَّة 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 لأيّ شخص من أيّ مكان وفي أي وقت الوصول إلى الأنظمة والأجهزة. يجب تنفيذ إجراءات الحماية المادية والمنطقية للسماح للموظفين المُخوَّلين فقط بالوصول إلى الأنظمة.
- يجب على المؤسسة تثبيت أنظمة المراقبة بحيث يتمّ تنبيهها على أيّ نشاطات غير طبيعية في النظام، أو أخطاء في النقل، أو معاملات استثنائية عبر الإنترنت. ويجب على المؤسسة إنشاء عملية متابعة للتحقق من أنّ هذه القضايا أو الأخطاء يتمّ تناولها بشكل مناسب في وقت لاحق.
- يجب أن تُحافظ 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 وتتبُّعه، فضلًا 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 للتصديق 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 تُقدِّم أنظمتها المالية عبر الإنترنت لتخدم المستثمرين المؤسسيين والمستثمرين المفوّضين أو الشركات، إذ يتمّ 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، فضلًا 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 النقّال**

- تشير خدمات الإنترنت عبر الهاتف النقّال إلى توفير الخدمات المالية عبر الأجهزة المحمولة مثل الهواتف النقّالة أو الأجهزة اللوحية. قد يختار الزبائن الوصول إلى هذه الخدمات المالية عبر متصفحات الويب على الهواتف الجوالة أو التطبيقات المطوَّرة ذاتيًّا على منصات الهواتف النقّالة مثل أنظمة تشغيل Apple iOS وGoogle Android وMicrosoft Windows.
- يشير الدفع بوساطة الهاتف النقّال 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 تُقدِّمها المؤسسات المصرفية ويمكن الوصول إليها من الإنترنت عبر أجهزة الكمبيوتر أو أجهزة الكمبيوتر المحمولة. ويجب على المؤسسة أيضًا تطبيق إجراءات أمنية مماثلة لتلك التي تُطبَّق على أنظمة الدفع المالي، والدفع من الإنترنت على خدمات المحمول عبر الإنترنت وأنظمة الدفع، ويجب أيضًا إجراء تقييم للمخاطر لتحديد سيناريوهات الاحتيال المحتملة ووضع التدابير المناسبة لمواجهة عمليات احتيال بطاقات الدفع عبر الأجهزة المحمولة.
- نظرًا إلى أنّ أجهزة الهاتف المحمول معرّضة للفقدان والسرقة، فيجب على المؤسسة التأكد من وجود إجراءات الحماية الكافية للمعلومات الحسّاسة والسرية المستخدمة في الخدمات وعمليات الدفع من خلال الإنترنت ويجب أن يكون لدى المؤسسة معلومات حسّاسة 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 تسبب أضرارًا شديدة ولها عواقب مؤذية.
- يجب حماية الأجهزة المرتبطة بأنظمة المدفوعات (ACH,RTGS) وخاصة الأجهزة الخاصة بنقل ملفات الـ(STP) بين النظام المحاسبي الشامل وأنظمة المدفوعات.

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

- تتيح بطاقات الدفع لحامليها المرونة لإجراء عمليات الشراء أينما كانوا. قد يختار حاملو البطاقات إجراء عمليات الشراء عن طريق تقديم هذه البطاقات فعليًّا للدفع لدى المتاجر، أو يمكنهم اختيار شراء حاجياتهم عن طريق الإنترنت، أو 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 تسلُّم البطاقة ("CNR") وحالات عدم عرض البطاقة ("CNP").

**الاحتيالات المُتعلِّقة ببطاقات الدفع**

- يجب على المؤسسة الذي يُقدِّم خدمات بطاقات الدفع أن تُقدِّم ضمانات كافية لحماية البيانات الحساسة لبطاقات الدفع. وينبغي التأكد من تشفير البيانات الحساسة للبطاقة لضمان سرية وسلامة هذه البيانات في التخزين والنقل، وتتمُّ معالجة المعلومات السرية في بيئة آمنة.
- يجب على المؤسسة نشر رقائق آمنة لتخزين البيانات الحساسة للبطاقة. ويجب أيضًا تنفيذ أساليب تصديق قوية للبطاقات، مثل أساليب تصديق البيانات الديناميكية ("DDA")، أو أساليب تصديق البيانات المدمجة ("CDA") لعمليات البطاقات عبر الإنترنت أو من دون إنترنت. وفيما يخص المعاملات التي يُنفّذها الزبائن ببطاقات الصراف الآلي الخاصة بهم، يجب أن تسمح المؤسسة فقط بتصريح المعاملات عبر الإنترنت، ويجب على جهة إصدار البطاقة وليس مُقدِّم الخدمة معالجة عمليات الدفع للجهات الخارجية وإجراء التصديق على المعلومات الثابتة الحسّاسة للزبائن مثل أرقام التعريف الشخصية أو كلمات المرور. وينبغي إجراء مراجعات أمنية منتظمة للبنية التحتية والعمليات التي يستخدمها زبائن مُقدِّمي هذه الخدمة.
- يجب أن يتمّ تنفيذ ضوابط الأمان في أنظمة وشبكات بطاقات الدفع.
- يجب على المؤسسة إرسال بطاقات الدفع الفعّالة 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 بـ(عدم عرض البطاقة CNP).
- لتعزيز حماية بطاقات الدفع يجب على المؤسسة فورًا إبلاغ حاملي البطاقات من خلال التنبيهات عندما تتجاوز السحوبات/ الرسوم المُحدَّدة للعميل. وأن تتضمّن هذه التنبيهات معلومات مثل المصدر وقيمة المعاملة.
- يجب على المؤسسة وضع أنظمة كشف الاحتيال المتينة ذات الأهداف السلوكية أو ما يعادلها؛ وقدرات الترابط لتحديد ومنع النشاطات الاحتيالية. ويجب أن تُحدِّد مقاييس إدارة المخاطر وفقًا للمخاطر التي يتعرض لها حاملو البطاقات أو طبيعة المعاملات أو عوامل الخطر الأخرى لتعزيز قدرات كشف الاحتيال.
- يجب على المؤسسة متابعة العمليات التي تُظهر انحرافًا 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**

- يوافر وجود أجهزة الصراف الآلي وأكشاك الدفع (على سبيل المثال، أجهزة SAM وAXS)، لحاملي البطاقات سهولة سحب النقود وعمليات سداد الفواتير، ومع ذلك فإنّ هذه الأنظمة هي أهداف إذ يتمّ 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 المناسب.
- 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 تتمّ في هذه الأجهزة والأكشاك والحفاظ على جودة التسجيلات.

يجب أن تتحقق المؤسسة من تنفيذ إجراءات الأمان المادية المناسبة في أكشاك الدفع الخاصة بالشركات الأخرى التي تقبل بطاقات دفع المؤسسة وتعالجها.

# المرفقات

## مرفق رقم (1)

## مصفوفة الأهداف المؤسسية (Enterprise goals)

| | | |
|---|---|---|
| 01 | تحقيق القيمة المضافة من موجودات واستثمارات المؤسسة | • نسبة الموجودات والاستثمارات التي حققت توقعات ذوي المصلحة بشأن القيمة المضافة<br>• نسبة المنتجات والخدمات التي حققت المنافع المرجوة منها<br>• نسبة الاستثمارات 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<br>• نسبة المنتجات والخدمات التي حققت رضا الزبائن<br>• نسبة المنتجات والخدمات التي حققت ميزة تنافسية في السوق |
| 03 | إدارة المخاطر الكلية المؤسسية (حماية الموجودات) | • نسبة الأهداف والخدمات الرئيسة المشمولة بعمليات تقييم المخاطر<br>• عدد الحوادث الرئيسة غير المحددة ضمن عمليات تقييم المخاطر من مجموع الحوادث الكلي<br>• تحديث دوري لملف المخاطر |
| 04 | الامتثال للقوانين والضوابط | • كلفة عدم الامتثال للقوانين والضوابط، بما يشمل الغرامات والتسويات<br>• عدد الموضوعات المخالفة للقوانين والضوابط التي سببت رأيًا عامًا سلبيًا تجاه المؤسسة أو سمعة سيئة<br>• عدد الموضوعات المخالفة لشروط التعاقد مع الغير |
| 05 | الإفصاح والشفافية المالية | • نسبة الموجودات والاستثمارات التي تمّ تحديدها والموافقة على موازناتها وعوائدها المتوقعة<br>• نسبة تكاليف الخدمات الممكن توزيعها على المستخدمين<br>• نسبة الرضا التي حققت المُتوقّع من قبل ذوي المصلحة فيما يخص الشفافية المالية، والدقة والفهم للبيانات المالية |
| 06 | ثقافة مؤسسية خدمية موجّهة للزبائن | • عدد حوادث الانقطاع للخدمات المصرفية والمالية بسبب حوادث مُتعلّقة بتقنية المعلومات والاتصالات<br>• نسبة رضا ذوي المصلحة على الخدمات والمنتجات المُقدّمة<br>• عدد شكاوى الزبائن |

## مرفق رقم (1)

## مصفوفة الأهداف المؤسسية (Enterprise goals)

| | | |
|---|---|---|
| 07 | استمرارية الخدمات وتوافرها | • عدد حوادث توقف الخدمات الرئيسة والحرجة<br>• تكاليف حوادث توقف العمليات والخدمات<br>• عدد ساعات توقف العمليات والخدمات<br>• نسبة الشكاوى المُتعلِّقة بتوقف الخدمات والعمليات |
| 08 | سرعة التغيير استجابة لمتطلبات بيئة العمل | • مستوى رضا المجلس عن سرعة الاستجابة للمتطلبات الجديدة<br>• عدد الخدمات والمنتجات المُقدَّمة من عمليات جديدة مستحدثة<br>• متوسط الزمن المستغرق للبدء بتحقيق أهداف استراتيجية موافق عليها |
| 09 | منهجية لصنع قرار مبني على المعلومات | • درجة رضا المجلس والإدارة التنفيذية العليا على عمليات صنع القرار<br>• عدد الحوادث الناتجة عن قرارات خاطئة بسبب الارتكاز على معلومات غير دقيقة<br>• الزمن المستغرق لتوفير المعلومات اللازمة لصنع القرار |
| 10 | تقليل تكاليف الخدمات والمنتجات | • الاتجاه الزمني للتكاليف بالمقارنة مع مستوى الخدمات<br>• تقييم دوري لتكاليف الخدمات المُقدَّمة<br>• مستوى رضا المجلس والإدارة التنفيذية العليا تجاه تكاليف الخدمات المُقدَّمة |
| 11 | تحسين مستوى الخدمات المُقدَّمة | • تقييم دوري لمستوى النضوج للخدمات المُقدَّمة<br>• نتائج واتجاه التقييم لمستوى النضوج<br>• رضا المجلس والإدارة التنفيذية العليا على كفاءة عمليات المؤسسة |
| 12 | تقليل تكاليف عمليات المؤسسة | • تقييم دوري لتقليل تكاليف العمليات<br>• الاتجاه الزمني للتكاليف بالمقارنة مع مستوى الخدمات<br>• مستوى رضا مجلس والإدارة التنفيذية العليا على تكاليف العمليات |

## مرفق رقم (1)

## مصفوفة الأهداف المؤسسية (Enterprise goals)

| | | |
|---|---|---|
| 13 | إدارة برامج التغيير للأعمال | • عدد البرامج المنجزة فيالوقت المخطط له والموازنات المُقدَّرة مسبقًا<br>• نسبة رضا ذوي المصالح عن البرامج المنجزة<br>• نسبة المعرفة والوعي بتغييرات الأعمال نتيجةً لمبادرات تقنية المعلومات والاتصالات |
| 14 | إنتاجية تشغيلية وعمالية | • عدد البرامج/ المشاريع المنجزة بالوقت وبالموازنات المرصودة<br>• مستويات التكاليف والعمالة المشغلة مقارنة بالمستهدفات |
| 15 | الامتثال للسياسات الداخلية | • عدد الحوادث الناتجة بسبب عدم الامتثال للسياسات الداخلية<br>• نسبة ذوي المصلحة وذوي المعرفة والوعي بالسياسات الداخلية<br>• نسبة السياسات المُفعّلة في المؤسسة |
| 16 | موظفون ذوو مهارة | • مستوى رضا ذوي المصلحة عن خبرات ومهارات الموظفين<br>• نسبة الوظائف المشغولة بأقل من المهارات والخبرات والمعارف المطلوبة<br>• مستوى الرضا الوظيفي |
| 17 | ثقافة تميّز وإبداع | • مستوى المعرفة والوعي بفرص الإبداع والتميز<br>• رضا ذوي المصلحة تجاه مستوى التميز والإبداع والأفكار المطروحة<br>• 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 مدى تحقق الأهداف | أرقام الأهداف المؤسسية ذات الصلة المباشرة |
|---|---|---|---|
| 01 | توافق الخطة الاستراتيجية لتقنية المعلومات والاتصالات مع الخطة الاستراتيجية للمؤسسة، من خلال اتّباع منهجية لصنع القرار الاستراتيجي للمؤسسة، كفوءة وتلبي متطلبات بيئة العمل الداخلية والخارجية | • نسبة أهداف المؤسسة الاستراتيجية المدعومة بأهداف تقنية المعلومات والاتصالات الاستراتيجية<br>• مستوى الرضا من قبل وحدات المؤسسة على محفظة المشاريع والخدمات المُخطَّط لتنفيذها ومدى تحقيقها للمتطلبات بكفاءة وفعّالية، ويمكن قياسه من خلال اتّباع أسلوب الاستبيان على سبيل المثال لا الحصر | 01,03,05,07,11,13 |
| 02 | امتثال ممارسات تقنية المعلومات والاتصالات ومساهمتها في امتثال المؤسسة للقوانين والأنظمة والضوابط المرعية | • تكلفة عدم امتثال تقنية المعلومات والاتصالات بما في ذلك تكاليف التصحيح المطلوبة، فضلًا عن مدى التأثير في سمعة المؤسسة بهذا الشأن<br>• عدد ملحوظات عدم الامتثال لمتطلبات تقنية المعلومات والاتصالات المرفوعة لمجلس الإدارة أو تلك التي تثير الرأي العام بشأنها | 01,05,07,09,12,17 |
| 03 | الالتزام من قبل الإدارة باتخاذ قرارات مبنية على معطيات تقنية المعلومات والاتصالات | • نسبة المهام والواجبات المُتعلِّقة بتقنية المعلومات والاتصالات من إجمالي المهام والواجبات للوصف الوظيفي لوظائف المؤسسة<br>• عدد المرات التي يتمّ فيها مناقشة موضوعات مُتعلِّقة بتقنية المعلومات والاتصالات في اجتماعات مجلس الإدارة<br>• اجتماعات 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 والاتصالات والمشمولة ضمن عمليات تقييم المخاطر<br>• عدد حوادث تقنية المعلومات والاتصالات الرئيسة التي لم تؤخذ بالحسبان لدى تقييم المخاطر<br>• نسبة العمليات التي تحتوي مخاطر تقنية المعلومات إلى مجموع العمليات المشمولة ضمن تقييم المخاطر<br>• دورية تحديث ملف المخاطر (Risk profile) | 02,10 |

## مرفق رقم (2)

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

| | | | |
|---|---|---|---|
| 05 | ضمان تحقيق المنفعة والقيمة المضافة من محفظة موارد تقنية المعلومات والاتصالات ومشاريعها وخدماتها | • نسبة مشاريع تقنية المعلومات والاتصالات التي تمّ فيها مراقبة وقياس المنافع والقيمة المضافة خلال مدّة عمر المشروع<br>• نسبة مشاريع تقنية المعلومات والاتصالات والخدمات التي حققت المنافع والنتائج المستهدفة وتلك التي تجاوزت المستهدفات | 06 |
| 06 | الشفافية في الإفصاح عن تكاليف تقنية المعلومات والاتصالات ومنافعها ومخاطرها | • نسبة المشاريع في المؤسسة التي تمّ فيها تحديد مصاريف تقنية المعلومات والاتصالات ونتائجها المتوقعة، والموافقة عليها.<br>• مستوى الرضا المسموح به عن مستوى الإفصاح والفهم والدقة للمخصصات المالية للمشاريع وخدمات تقنية المعلومات والاتصالات | 01,07 |
| 07 | تقديم خدمات تقنية المعلومات والاتصالات التي تلبي متطلبات عمليات المؤسسة | • عدد مرات توقف عمليات المؤسسة بسبب حوادث وانقطاع خدمات تقنية المعلومات والاتصالات<br>• مستوى الرضا من قبل أقسام المؤسسة على قيام إدارة تقنية المعلومات والاتصالات بتحقيق متطلبات العمل في الوقت والمواصفات المتفق عليها ضمن اتفاقيات مستوى الخدمات الخارجية والداخلية | 04,10,14 |
| 08 | الاستخدام المناسب للبرمجيات وحلول تقنية المعلومات والاتصالات | • نسبة مسؤولي عمليات المؤسسة الراضين عن منتجات وخدمات تقنية المعلومات والاتصالات<br>• مستوى فهم مسؤولي عمليات المؤسسة لخصائص البرمجيات وحلول تقنية المعلومات والاتصالات على دعم عملياتهم<br>• مستوى الرضا عن التدريب المُقدَّم لمستخدمي تقنية المعلومات والاتصالات، وعن مدى كفاية دليل استخدام البرمجيات والحلول المختلفة | 01, 07, 09, 17 |
| 09 | رشاقة عمليات تقنية المعلومات والاتصالات وإدارة مواردها | • مستوى رضا مسؤولي المؤسسة على مستوى الاستجابة لمتطلباتهم من تقنية المعلومات والاتصالات<br>• عدد عمليات المؤسسة المخدومة من قبل موارد حديثة لتقنية المعلومات والاتصالات<br>• الوقت المتوسط المستغرق لترجمة الهدف الاستراتيجي لمفردات مبادرة تقنية المعلومات والاتصالات | 14 ,01 |
| 10 | أمن المعلومات، تشغيل البرمجيات والبنية التحتية لتقنية المعلومات والاتصالات | • عدد حوادث أمن المعلومات التي تسببت بخسائر مالية أو إنقطاع في العمليات أو التأثير في السمعة<br>• عدد خدمات تقنية المعلومات والاتصالات المُحدَّدة فيها المتطلبات الأمنية لتقنية المعلومات والاتصالات<br>• المدّة الزمنية اللازمة لإجراءات التعديلات المطلوبة على مستوى امتيازات النفاذ للمستخدمين<br>• تقييم دوري لمعطيات أمن المعلومات بحسب أحدث المعايير الدولية المقبولة | 04,06,11 |

## مرفق رقم (2)

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

| | | | |
|---|---|---|---|
| 11 | الاستغلال الأمثل لموارد وقدرات تقنية المعلومات والاتصالات | • تقييم دوري لدرجة النضوج وتكاليف موارد تقنية المعلومات والاتصالات<br>• نتائج واتجاه التقييم أعلاه<br>• مستوى الرضا من قبل إدارة المؤسسة ككل على قدرات تقنية المعلومات والاتصالات وعلى حجم التكاليف | 01,07,08,09,12 |
| 12 | دعم آليات العمل من خلال تكامل البرمجيات التطبيقية وموارد التقنية ضمن عمليات المؤسسة | • عدد الحوادث الناتجة بسبب أخطاء تكامل البرمجيات<br>• عدد حوادث تعطل عمليات المؤسسة بسبب تعطل برمجيات وتقنية المعلومات والاتصالات<br>• عدد مرات تعطل مشاريع أو تأخرها بسبب البنية التحتية ومشاكل تقنية المعلومات والاتصالات<br>• عدد البرمجيات والحلول غير المتكاملة، والتي تعمل بمعزل عن باقي البرمجيات والحلول | 05,06,11 |
| 13 | تنفيذ المشاريع ضمن الزمن والموازنات المالية المُحدَّدة مسبقًا ضمن إطار إدارة محفظة للمشاريع تتوافق والقواعد والمعايير الدولية المتبعة بهذا الشأن | • عدد المشاريع المُنفَّذة ضمن حدود الزمن والموازنة المرصودة<br>• نسبة الرضا من قبل ذوي المصلحة عن جودة إدارة المشاريع<br>• عدد المشاريع التي تتطلّب إعادة بسبب ضعف الجودة في الأداء وتحقيق الأهداف<br>• نسبة تكاليف الصيانة إلى إجمالي تكاليف تقنية المعلومات والاتصالات | 01,03,13 |
| 14 | توافرية معلومات معتمد عليها ومفيدة مرتكز عليها في اتخاذ القرار | • مستوى رضا دوائر المؤسسة على جودة المعلومات وتوافريتها<br>• عدد حوادث عمليات المؤسسة بسبب قلة توافرية المعلومات والتقنية<br>• نسبة أهمية قرارات المؤسسة الخاطئة بسبب قلة توافرية المعلومات والتقنية | |
| 15 | امتثال ممارسات تقنية المعلومات والاتصالات للسياسات الداخلية للمؤسسة | • عدد حوادث تقنية المعلومات والاتصالات نتيجة عدم الامتثال للسياسات<br>• نسبة الأفراد ذوي الفهم الصحيح للسياسات<br>• نسبة السياسات التي تحاكي أفضل الممارسات الدولية<br>• دورية مراجعة وتحديث السياسات | |
| 16 | مستوى المهارات والتنافسية لكوادر المؤسسة بشكل عام وكوادر تقنية المعلومات والاتصالات | • نسبة الموظفين الذين لديهم مهارات تقنية معلومات كافية لمتطلبات العمل<br>• نسبة رضا الموظفين للمهام المُتعلِّقة بتقنية المعلومات والاتصالات المنوطة بهم<br>• عدد ساعات التدريب والتعلُّم للموظف | |
| 17 | امتلاك المعرفة والخبرة في الابتكارات التقنية الممكن توفيرها لتطوير عمليات المؤسسة | • مستوى المعرفة في عمليات المؤسسة والابتكارات التقنية الممكن توفيرها لدعم تلك العمليات | |

# مرفق (3)

## عمليات حوكمة تقنية المعلومات والاتصالات

| 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 تقنية المعلومات والاتصالات وتحديثه | تحليل وتوضيح متطلبات حوكمة تقنية المعلومات والاتصالات ووضع سياسات عمل تقنية المعلومات والاتصالات ومبادئه وإجراءاته، والهياكل التنظيمية ذات العلاقة، والاستمرار بتطويرها وتحديثها مع تحديد واضح للمسؤوليات والصلاحيات الكفيلة بتحقيق أهداف المؤسسة | إيجاد منهجية متكاملة تتوافق والإطار العام للحوكمة المؤسسية، لضمان أخذ قرارات تقنية المعلومات والاتصالات تتماشى مع تحقيق الأهداف الاستراتيجية للمؤسسة، وإنّ عمليات تقنية المعلومات والاتصالات مراقبة بكفاءة وشفافية عاليتين ضمن إطار الامتثال لاستراتيجية 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 والاتصالات المُوظَّفة بكلف مقبولة | الاستغلال الأمثل وتعظيم حجم المنافع من موارد تقنية المعلومات والاتصالات بأقل التكاليف الممكنة بما يلبي ويحقق متطلبات العمل | 01,05,06,07,17 |
| EDM 03 | ضمان إدارة صحيحة لمخاطر تقنية المعلومات والاتصالات | الفهم السليم للمخاطر من حيث القابلية على تحمّل المخاطر (Risk appetite) ودرجة تحمّل المخاطر (Risk tolerance)، وتبرير القيمة المضافة، والمنافع من وراء قبول تلك المخاطر، فضلًا عن توضيح وتوثيق وتوصيل تلك القواعد لذوي العلاقة | ضمان عدم تجاوز مخاطر تقنية المعلومات والاتصالات من حيث قابلية تحمّلها ودرجة تحمّل المخاطر المُحدَّدتين، وضمان تحديد وإدارة مخاطر تقنية المعلومات والاتصالات وتقليل احتمالية مخالفة القوانين والأنظمة والضوابط | 04,06,10,15 |
| EDM 04 | ضمان الاستغلال الأمثل لموارد تقنية المعلومات والاتصالات | ضمان ملاءمة وتوافر موارد العمليات وتقنية المعلومات والاتصالات (العنصر البشري، وإجراءات العمل، والتقنية) لتلبية أهداف المؤسسة بكفاءة، بأقل الكلف الممكنة | ضمان الاستغلال الأمثل للموارد بما في ذلك موارد تقنية المعلومات والاتصالات، وأنّ هناك زيادة محتملة في المنافع المحققة | 09,11,16 |

## مرفق (3)

## عمليات حوكمة تقنية المعلومات والاتصالات

| 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 والاتصالات، والتأكد من تحديد والموافقة على الأهداف والمعايير الخاصة بالإجراءات التصحيحية بهذا الشأن | التأكد من وصول تقارير قياس الأداء لموارد تقنية المعلومات والاتصالات لذوي العلاقة في الوقت اللازم؛ بهدف تحسين مستوى الأداء، وتحديد المواضع التي تكون بحاجة إلى تحسين وعناية، والتأكد من أنّ أهداف تقنية المعلومات والاتصالات تتماشى والأهداف الاستراتيجية للمؤسسة | 03,06,07 |
| **عمليات التوافق والتخطيط والتنظيم Align,plan and Orgnize (APO)** | | | | |
| APO 01 | تفعيل الإطار العام لإدارة تقنية المعلومات والاتصالات | التوضيح والاستمرار بتحديث الرؤية والرسالة بشأن حوكمة تقنية المعلومات والاتصالات، والاستمرار في توظيف آليات العمل وتفويض الصلاحيات اللازمة لإدارة المعلومات باستخدام تقنيات لتحقيق أهداف المؤسسة ضمن إطار الالتزام بالمبادئ والسياسات | استخدام منهجية إدارية متناسقة لتحقيق متطلبات حوكمة تقنية المعلومات والاتصالات تشمل كُلّ من الهياكل التنظيمية المطلوبة، والأدوار والمسؤوليات والنشاطات والعمليات، والمهارات والخبرات | 01,02,09,11, 15,16,17 |
| APO 02 | إدارة الاستراتيجية Manage strategy | تقديم وصف شامل للوضع الحالي للمؤسسة ولبيئة تقنية المعلومات والاتصالات وتحديد التوجه المستقبلي متضمنًا المبادرات المطلوبة للانتقال لبيئة العمل المستقبلية، وتوظيف موارد وقدرات المؤسسة والخدمات المُقدّمة والمستعان بها من قبل الغير بفعالية واعتمادية عاليتين لتحقيق الأهداف الاستراتيجية للمؤسسة | مواءمة الأهداف الاستراتيجية لتقنية المعلومات والاتصالات لتلبية تحقيق أهداف المؤسسة، وتحديد المسؤوليات تجاه تحقيق الأهداف بوضوح، والتأكد من الفهم الصحيح لها من قبل ذوي المصلحة | 01,07,17 |

# مرفق (3)

## عمليات حوكمة تقنية المعلومات والاتصالات

| رمز العملية | عنوان العملية | وصف العملية | هدف العملية | أرقام وأهداف المعلومات والتقنية المصاحبة لها ذات الصلة المباشرة |
|---|---|---|---|---|
| APO 03 | إدارة هيكلية تقنية المعلومات والاتصالات Manage Enterprise Architecture | إنشاء الهيكل العام لإدارة تقنية المعلومات والاتصالات بما في ذلك عمليات المؤسسة والمعلومات والبيانات والبرامج والبنية التحتية لتقنية المعلومات والاتصالات بغرض تحقيق أهداف التقنية وأهداف المؤسسة الاستراتيجية بكفاءة وفعالية، من خلال إنشاء نماذج وممارسات عمل رئيسة، وتحديد المتطلبات اللازمة لايجاد مجموعة من المبادئ والإجراءات والأدوات المترابطة مع بعضها البعض، والعمل على تحسين مستوى التوافق بين التقنية ومتطلبات عمل المؤسسة، وزيادة رشاقة خدمات تقنية المعلومات والاتصالات، وتحسين جودة المعلومات والتقنية المعتمد عليها في تسيير عمليات المؤسسة | تحديد المعطيات المختلفة اللازمة لبناء إدارة تقنية المعلومات والاتصالات، وتحديد المبادئ والإجراءات المستخدمة في ذلك وتوصيف العلاقات بينهما للوصول إلى الأهداف التشغيلية والاستراتيجية للمؤسسة | 01,09,11 |
| APO 04 | إدارة الابتكارات Manage Innovation | زيادة الوعي بما هو معروض من جديد في سوق تقنية المعلومات والاتصالات لدراسة إمكانية استغلال ذلك لدعم عمليات المؤسسة الحالية والمبتكرة لخدمة تحقيق أهداف المؤسسة الاستراتيجية | تحقيق الميزة التنافسية للمؤسسة من خلال تطوير وزيادة كفاءة وفعالية عمليات المؤسسة استنادًا إلى جديد تقنية المعلومات والاتصالات | 05,08,09,11.17 |

## مرفق (3)

## عمليات حوكمة تقنية المعلومات والاتصالات

| 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 الموارد ومن ثَمَّ الاستغلال الأمثل لها، والعمل على تقييم وترتيب أولوية المشاريع وفقًا 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 حينه استنادًا 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 والكلفة Manage budget and cost | إدارة الشؤون المالية لموارد تقنية المعلومات والاتصالات من خلال آليات عمل كُلّ من الإدارة المالية وإدارة تقنية المعلومات والاتصالات في المؤسسة، بما في ذلك إعداد الموازنات ودراسة الكلف والمنافع وترتيب أولويات من خلال استخدام أُسس ومعايير موضوعية موحدة معتمدة في المؤسسة بهذا الشأن، والعمل بالتشاور مع 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 لموارد التقنية وتقديم المعلومات بهذا الشأن بشفافية عالية تسهّل عمليات المساءلة وتقدير حجم المنافع والقيمة المضافة، وتسهيل آليات اتخاذ القرار في توظيف موارد تقنية المعلومات والاتصالات | 05,06 |

# مرفق (3)

## عمليات حوكمة تقنية المعلومات والاتصالات

| 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 ايجاد الهياكل التنظيمية وخطوط الاتصال المؤسسي الافقي والعمودي،وتوظيف العنصر البشري الماهر والكفوء وتوزيع الصلاحيات والمهام والأدوار والمسؤوليات،وايجاد خطط التدريب والتعلم المستمر،وتحفيز الموظفين بشكل دائم للحصول على الاداء المطلوب | الاستغلال الأمثل للموارد البشرية لخدمة أهداف المؤسسة | 01,11,13,16,17 |
| APO 08 | إدارة العلاقات Manage relationship | إدارة العلاقات بين دائرة تقنية المعلومات والاتصالات وباقي ادارات 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 الايجابية في المبادرة باتخاذ القرارات وتحمل المسؤوليات حيالها | تحسين النتائج وزيادة مستوى الثقة والاعتماد الكفوء لموارد تقنية المعلومات والاتصالات | 01,07,12,17 |
| APO 09 | إدارة اتفاقيات الخدمات Manage service agreements | توافق مستوى جودة الخدمات المُتعلِّقة بتقنية المعلومات والاتصالات مع توقعات واحتياجات المؤسسة بما في ذلك آليات تعريف وتحديد وتصميم وطلب تلك الخدمات وتوثيق التعاقدات مع الغير بشأنها، ووضع المعايير للمراقبة المستمرة لجودة ومستوى تلك الخدمات | التأكد من أنّ خدمات تقنية المعلومات والاتصالات المُقدَّمة على مستوى من الجودة وتلبي احتياجات المؤسسة الحالية والمستقبلية | 07,14 |

# مرفق (3)

## عمليات حوكمة تقنية المعلومات والاتصالات

| رمز العملية | عنوان العملية | وصف العملية | هدف العملية | أرقام وأهداف المعلومات والتقنية المصاحبة لها ذات الصلة المباشرة |
|---|---|---|---|---|
| APO 10 | إدارة المزوّدين Manage suppliers | إدارة خدمات تقنية المعلومات والاتصالات المُقدَّمة من قبل الغيرلدعم عمليات وأهداف المؤسسة، بما في ذلك آليات اختيار المزوّدين والاتصال بهم وإدارة التعاقدات معهم ومراقبة وتقييم أدائهم لفحص مدى الكفاءة والفعالية والامتثال للشروط التعاقدية معهم | تقليل مستوى المخاطر قدر الإمكان نتيجة للاستعانة بالخدمات المُقدَّمة 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 احتياجات العمل وتلقى 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 امن المعلومات Manage security | تعريف وتشغيل ومراقبة نظام إدارة أمن المعلومات | الحفاظ على حجم تأثيرواحتمالية حدوث متوقعة لحوادث تقنية المعلومات والاتصالات ضمن مستويات مقبولة لمدى تقبل المؤسسة على تحمل المخاطر | 02,04,06,10,14 |

# مرفق (3)

## عمليات حوكمة تقنية المعلومات والاتصالات

| رمز العملية | عنوان العملية | وصف العملية | هدف العملية | أرقام وأهداف المعلومات والتقنية المصاحبة لها ذات الصلة المباشرة |
|---|---|---|---|---|
| عملية البناء (التطوير) والشراء والتشغيل Build, acquire and implement (BAI) | | | | |
| BAI 01 | إدارة البرامج والمشاريع Manage programmes and projects | إدارة جميع مشاريع المؤسسة لتحقيق الأهداف الاستراتيجية بشكل تعاوني بين إدارة تقنية المعلومات والاتصالات وباقي الإدارات المعنيّة، 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 والاحتياجات 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 تلبي احتياجات العمل بأقل المخاطر | 01,07,12 |

# مرفق (3)

## عمليات حوكمة تقنية المعلومات والاتصالات

| 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 تلبي متطلبات العمل واحتياجاته، تشمل آليات تصميم وتطوير وشراء والاستعانة بالغير. تشمل إدارة التعريفات (configuration 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 الاستيعابية manage availability and capacity | عمل التوازن المطلوب بتوفير خدمات تقنية المعلومات والاتصالات بين الحاضر والمستقبل مع الأخذ بالحسبان الكلف ومستوى الأداء، بما في ذلك تحديد القدرات الحالية والمستقبلية استنادًا 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 enablement | تحسين احتمالية نجاح عمليات التغيير المؤسسي بسرعة وبأقل المخاطر بما يشمل آليات التغيير وعمليات المؤسسة وتقنية المعلومات والاتصالات والأفراد | إعداد وضمان الالتزام الافراد بالتغيير المؤسسي بنجاح وبأقل المخاطر | 08,13,17 |

## مرفق (3)

## عمليات حوكمة تقنية المعلومات والاتصالات

| رمز العملية | عنوان العملية | وصف العملية | هدف العملية | أرقام وأهداف المعلومات والتقنية المصاحبة لها ذات الصلة المباشرة |
|---|---|---|---|---|
| BAI 06 | إدارة التغييرات Manage changes | إدارة التغييرات كافّة من خلال توفير الضوابط اللازمة من مبادئ وسياسات التغيير تشمل التغييرات الطارئة والمستعجلة والتغيير على عمليات المؤسسة والبرامجيات والبنية التحتية للتقنية، فضلًا عن توفير معايير وإجراءات للتغيير تتضمن قياس أثر التغيير في العمليات، والأولويات في التغيير، والموافقات المطلوبة للتغيير وإجراءات التغييرات الطارئة، واستخراج تقارير التتبع للتغييرات، الإغلاق والتوثيق | إجراء التغييرات المطلوبة بالسرعة الممكنة وبأقل المخاطر المحتملة لأي آثار سلبية في مصداقية التغييرات | 04,07,10 |
| BAI 07 | إدارة قبول التغيير والانتقال 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 منظومة معارف محدّثة ومعتمد عليها والحفاظ 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 ورفع مستوى الإنتاجية | 09,17 |

## مرفق (3)

## عمليات حوكمة تقنية المعلومات والاتصالات

| رمز العملية | عنوان العملية | وصف العملية | هدف العملية | أرقام وأهداف المعلومات والتقنية المصاحبة لها ذات الصلة المباشرة |
|---|---|---|---|---|
| BAI 09 | إدارة الموجودات Manage assets | إدارة موجودات تقنية المعلومات والاتصالات على مدار دورة حياتها للتأكد من تحقيقها المنافع المرجوة بأقل التكاليف الممكنة، وبأنها تتناسب والعمليات المشغلة ضمنها، وبأنها معدودة ومحمية، وأنّ الموجودات المهمة لدعم العمليات المصرفية الحسّاسة متوافرة بشكل مستمر ومعتمد عليها، وإدارة تراخيص البرامجيات للتأكد من كفايتها لدعم عمليات المؤسسة وبأنّ استخدامها هو ضمن حدود القوانين المعتمدة بهذا الشأن | إدارة موجودات تقنية المعلومات والاتصالات والاستخدام الأمثل لها | 06,11 |
| BAI 10 | إدارة التكوين Manage configuration | وصف كُلّ من الموارد الرئيسة للمؤسسة من جهة وقدرات تقنية المعلومات والاتصالات المطلوبة لتقديم خدمات التقنية من جهة أُخرى وتعريف العلاقة بينهما، بما يشمل جمع معلومات المختلفة ووضع الأُسس المعيارية، وإخضاعها لعمليات المراجعة الدورية والتدقيق المستمر | توفير معلومات كافية عن خدمات وخصائص موجودات تقنية المعلومات والاتصالات لإدارة تلك الموجودات بكفاءة، ومعرفة أثر تغيير تلك الخصائص في العمل من ناحية أمن المعلومات والتقنية | 02,11,14 |
| **عمليات توصيل الخدمات والدعم Delivery, service and Support (DSS)** | | | | |
| DSS 01 | إدارة العمليات Manage operations | تنسيق وتنفيذ نشاطات 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 حوكمة تقنية المعلومات والاتصالات

| 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 Requests and Incidents | الاستجابة في الوقت المُحدَّد لطلبات المستخدمين ولكل أنواع حوادث تقنية المعلومات والاتصالات، إعادة تشغيل العمليات التقنية بعد الانقطاعات، وتوثيق طلبات المستخدمين، وإجراء التحقيقات اللازمة لاختراقات التقنية وتشخيصها وإعلام الإدارة المعنية بشأنها ومعالجتها | رفع مستوى الإنتاجية وتقليل معدل الانقطاعات من خلال الاستجابة السريعة لطلبات المستخدمين ومعالجة حوادث تقنية المعلومات والاتصالات | 04,07 |
| DSS 03 | إدارة المشاكل Manage problems | تحديد وتصنيف أعطال تقنية المعلومات والاتصالات بما في ذلك مسبباتها الرئيسة 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 الاستمرارية Manage continuity | إنشاء خطة لإدارة استمرارية عمليات المؤسسة وتقنية المعلومات والاتصالات وتطويرها؛ لضمان استمرارية عمليات المؤسسة الحساسة والحرجة لمواجهة أسباب الانقطاع وحوادثه ضمن الحدود المستهدَفة 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 service | حماية معلومات المؤسسة والإبقاء عليها بمستوى مخاطر مقبول ضمن إطار سياسات أمن المعلومات وحمايتها للمؤسسة، وإنشاء والاستمرار بتحديث مهام ومسؤوليات إدارة أمن المعلومات، والامتيازات للنفاذ والاستخدام ومراقبة الاستخدام لموارد التقنية | تقليل الأثر السلبي في عمليات المؤسسة جَرَّاء الحوادث ونقط الضعف لأمن المعلومات | 02,04,10 |

## مرفق (3)

## عمليات حوكمة تقنية المعلومات والاتصالات

| 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 والاستمرار في توظيفها، الكفيلة بتحقيق المتطلبات الأمنية المُحدَّدة للمعلومات والتقنية المصاحبة لها، تلك العمليات سواء المُنفَّذة داخليًا 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, Evaluate and Assess (MEA)** | | | | |
| MEA 01 | مراقبة وتقييم وتقدير الأداء والمطابقة Monitor, Evaluate 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 تحقق المستهدفات بشأنها ورفع التقارير اللازمة بهذا الشأن دوريًا | الشفافية بشأن مستوى الأداء تجاه تحقيق الأهداف | 04,07,11,15 |
| MEA 02 | مراقبة نظام الضبط والرقابة الداخلية للمؤسسة وتقييمه وتقديره Monitor evaluate and asses the system of internal control | المراقبة المستمرة والتقييم لبيئة الضوابط الداخلية بوساطة كُلّ من التقييم الذاتي والتقييم المستقل، وتمكين الإدارة من تحديد الاختلالات في الضوابط المفعّلة لاتخاذ التحسينات والتصحيحات المطلوبة، التخطيط والتنظيم والتحديث لمبادئ وقواعد التقييم لنظام الضبط والرقابة الداخلي للمؤسسة | تقديم المعلومات بشفافية لذوي المصلحة بشأن مدى سلامة وملاءمة نظام الضبط والرقابة الداخلي لعمليات المؤسسة، في المساهمة بتحقيق أهداف المؤسسة من خلال الفهم الصحيح لمستويات المخاطر المتبقية في المؤسسة (residual risk) | 02,04,15 |

## مرفق (3)

## عمليات حوكمة تقنية المعلومات والاتصالات

| 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 التعاقدات مع الغير، والحصول على تأكيدات بتحديد المتطلبات القانونية والتعاقدية ومستوى الامتثال لها، وعد موضوع الامتثال لمتطلبات التقنية | التأكد من امتثال المؤسسة للقوانين والأنظمة والضوابط | 02,04 |

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

**(اسم المُدقِّق أو مؤسسة التدقيق)**

| |
|---|
| **تقرير تقييم (مخاطر – ضوابط) المعلومات والتقنية المصاحبة لها للمؤسسة/ لمصرف.....**<br><br>**الإدارة العامة (أو الإقليمية) – بغداد/ العراق (أو بلد الفرع)** |
| **مدّة التدقيق**<br>من تاريخ – إلى تاريخ<br>**عدد أيام العمل**<br>( ) يومًا |

| | |
|---|---|
| اسم المُدقِّق المسؤول | مع إرفاق ملحق عن المؤهلات والخبرات وصور عن الشهادات الأمنية والزمالات السارية |
| أسماء أعضاء فريق التدقيق | مع إرفاق ملحق عن المؤهلات والخبرات وصور عن الشهادات المهنية والزمالات السارية |

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

**أوّلًا: أنموذج إطلاع وتوصيات المجلس على التقرير:**

**ثانيًا: المُقدّمة: (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 () استنادًا إلى **محاور التقييم الآتية**، علمًا بأنّ درجات التقييم تُقسّم تنازليًا 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، وتمّ تقييمها بدرجة ().

ب- البرامج التطبيقية، وتمّ تقييمها بدرجة ().

ت- إدارة البيانات

ث- أجهزة الكمبيوتر الرئيسة وإدارتها، وتمّ تقييمها بدرجة ().

ج- الشبكات، وتمّ تقييمها بدرجة ().

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

2. **منهجية الفحص والتقييم :**

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

أ. **كمية المخاطر:**

تمّ احتسابها وتقديرها على أساس المعادلة الآتية:

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

أي: إنّ تقدير كمية المخاطر الحالية (Current Risk) تمّ بناءً على أهمية نقطة الضعف والتهديد الذي تُشكّله (الملحوظة) مع الأخذ بالحسبان المخففات المتمثلة بالضوابط المفعّلة. إذ تمّ تقسيم درجات كمية المخاطر تنازليًا على ثلاثة مستويات: (عالي، متوسط، منخفض) (من الممكن اختيار سُلّم تقييم أكثر تفصيلًا)، وتمّ تقسيم الأهمية (المقصود بها المخاطر الموروثة Inherent Risk) تنازليًا على أربعة مستويات (حرج، جوهري، متوسط، قليل)، وتمّ تقسيم قوة الضوابط تنازليًا على أربعة مستويات (ممتاز، جيد، ملائم، ضعيف). علما بأنه تمّ اتّباع **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 استنادًا إلى نوعية إدارة المؤسسة لمخاطر التشغيل من حيث توافر استراتيجية أو سياسة مخاطر مُقرّة من المجلس تُجسّد رؤية البنك، ومقدار الرغبة في تحمل المخاطر(Risk Appetite)، فضلًا 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 تجنّب المخاطر (Avoid)، أو رفض المخاطر (Reject). وقد تمّ تقسيم نوعية إدارة المخاطر تنازليًا على ثلاثة مستويات (قوي، مقبول، ضعيف) (من الممكن اختيار سُلّم تقييم أكثر تفصيلًا).

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

**وفيما يأتي جدول يلخص تقييم الملحوظات الواردة في متن التقرير، ويُحدِّد المسؤولية:**

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

3. **مناقشة التقارير:**

تمَّ بتاريخ // إرسال التقرير إلى إدارة المؤسسة تمهيدًا لعقد اجتماع مع الأطراف المعنيّة لمناقشة محتوياته، هذا وقد تمَّ بتاريخ // الاجتماع مع إدارة المؤسسة مُمثَّلة بكل من.....، وقد حقّق الاجتماع أهدافه من حيث:

أ. التأكد من مصداقية محتويات تقرير التدقيق.
ب. التأكد من الفهم الصحيح لمحتويات تقرير التدقيق من قبل إدارة المؤسسة.

الاتفاق على التواريخ الواجب على إدارة المؤسسة الالتزام بها لتصحيح الثغرات ونقط الضعف الواردة في تقرير التدقيق

4. **مُحدِّدات التدقيق:**

يتمُّ ذكر أية مُحدِّدات أثّرت سلبًا 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 المُدقِّق وتسهيل مهمته، وأية معيقات أو مُحدِّدات أخرى.

5. **مؤهلات وخبرات المحقق المسؤول وأعضاء فريق التحقيق:**

(يتمُّ ذكرها).

### ثالثًا: متن التقرير: ونعرض فيما يأتي تفاصيل التقييم في أعلاه:

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

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

تمَّ تقييمها بدرجة - يتمّ استخدام سُلَّم تقييم المخاطر Component Risk Rating المذكور في أعلاه ( Composite Risk Rating- وذلك على النحو الآتي:

**الملحوظة (١ : ١): حوكمة المعلومات والتقنية المصاحبة لها: (ذُكِرَت على سبيل المثال، ويتمّ توصيف باقي الملحوظات في المحور)**

| تقييم الملحوظة (1:1) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| مدى الأهمية | حرج | X | **جوهري** | | **متوسط** | | **قليل** | |
| تقييم الضوابط | ممتاز | | جيد | | ملائم | | ضعيف | X |
| كمية المخاطر | عالي | X | متوسط | | منخفض | | | |
| نوعية وإدارة المخاطر | قوي | | مقبول | | ضعيف | X | | |

## مرفق رقم (4): أنموذج تقرير تدقيق المعلومات والتقنية المصاحبة لها

يتمُّ توصيف الثغرات (Vulnerabilities) التي تُشكِّل نقط ضعف في الضوابط والأنظمة والإجراءات، فضلًا عن توصيف التهديدات (Threats) التي يمكن التعرُّض لها، وبالمحصلة يتمّ توصيف الأثر (Impact) سواء الأثر المالي أو التشغيلي أو القانوني أو أثر السمعة... إلخ.

**التوصية:**

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

**رد إدارة المؤسسة:**

يتمُّ ذكر ردّ إدارة المؤسسة

2. **. البرامج التطبيقية (Applications):-**

تمَّ تقييمها بدرجة ()، وذلك على النحو **الآتي**:

3. **إدارة البيانات (Data Management):**

تمَّ تقييمها بدرجة ()، وذلك على النحو **الآتي**:

4. **أجهزة الكمبيوتر الرئيسة بما فيها أنظمة التشغيل والبرمجيات الأخرى (Servers) :**

تمَّ تقييمها بدرجة ()، وذلك على النحو **الآتي**:

5. **شبكات الكمبيوتر المحلية والواسعة والإنترنت والإنترانت والأنظمة المساندة (Networks):**

تمَّ تقديمها بدرجة ()، وذلك على النحو **الآتي**:

6. **خطط الطوارئ وخطط استمرارية العمل، والحماية المادية والبيئية Business Continuity and disaster recovery plans, physical and environmental security**

تمَّ تقييمها بدرجة ()، وذلك على النحو **الآتي**:

**رابعا: جدول بالملحوظات العالقة ولم تُعالج 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 تقنية المعلومات والاتصالات IT Governance |
|---|
| مدى كفاية وكفاءة تحقيق عمليات حوكمة تقنية المعلومات والاتصالات، الواردة في المرفق رقم (٣)، وضوابط البنك المركزي العراقي المُتعلِّقة بهذا الشأن من خلال تطبيق عمليات الرقابة والتقييم والقياس (MEA) الواردة في المرفق المذكور آنفًا |
| مستوى التوافق الاستراتيجي بين أهداف تقنية المعلومات والاتصالات |
| مدى كفاية وفعالية السياسات الخاصة بأمن المعلومات وحمايتها |
| مستوى رضا المستخدمين على إدارة تقنية المعلومات والاتصالات والخدمات والمنتجات والدعم الفني المُقدَّم |
| مدى كفاية لجان تقنية المعلومات والاتصالات 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 والاتصالات |
| 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 والاتصالات 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 المشاريع Project Portfolio Management |
| مدى الامتثال لضوابط البنك المركزي العراقي والقوانين والتشريعات والأنظمة ذات العلاقة |
| مدى امتثال مجلس الإدارة والإدارة التنفيذية لضوابط حوكمة تقنية المعلومات والاتصالات |
| مدى استخدام أدوات وبرامج لكشف الاحتيال (CAATS) مثل (ACL,IDEA) من قبل التدقيق |

## مرفق (5)
## محاور تدقيق المعلومات والتقنية المصاحبة له

| |
|---|
| مدى وجود سياسات الاستعانة بالغير وكفايتها (التعهيد أو الاسناد) (Outsourcing) |
| مدى كفاية التوثيق للتعاقدات الخارجية والداخلية وملاحقها من حيث تفصيل الخدمات المُقدَّمة 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 تُعنى بآليات 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 الحساسة، والموافقة المسبقة عليها |
| فحص ضوابط إدخال البيانات على البرامج الحسّاسة مثل وجود (Maker,checker) |
| فحص ضوابط المخرجات والحفظ الآمن 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 الإلكتروني |
| 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 البنك المركزي العراقي بشأن التصنيف الآلي للتسهيلات |

# مرفق (5)
## محاور تدقيق المعلومات والتقنية المصاحبة له

| 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 المُصرَّح به من قبل ضابط قواعد البيانات |
| مدى كفاءة وتفعيل إجراءات النسخ الاحتياطي |
| مدى كفاءة وتفعيل عمليات مراقبة الاستخدام (DBA) من قبل إدارة منفصلة مثل أمن المعلومات |
| مدى كفاءة وتفعيل والاستناد إلى آليات 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 كُلّ تغيير (ترقية، تطوير) |
| مدى كفاءة وتفعيل إجراءات مراجعة تقارير متابعة الاستخدام لمديري الأنظمة (Administrators Logs)، وهل تُراجَع 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 |

# مرفق (5)

## محاور تدقيق المعلومات والتقنية المصاحبة له

| |
|---|
| مدى كفاءة إجراءات فحوصات الاختراق وتحديد الثغرات، وكفايتها ( vulnerability 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، وفعّاليتها |
| فحص مستوى التوافرية لعناصر الشبكات ومدى ملاءمتها لخطط استمرارية العمل |
| مدى كفاية إجراءات مراقبة الاستخدام للشبكات، وفعّاليتها (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 الـ ISO /OSI التي تعمل عليه (مثال على المستوى الثالث Network Layer، أو المستوى السابع Application Layer) ومدى كفاية معايير الأمن والحماية لسرية وخصوصية البيانات ومصداقيتها بصورة خاصة |
| مدى كفاية إجراءات إدارة منفصلة وفعّاليتها، مثل أمن المعلومات بمراجعة التعديلات الحاصلة على ( Firewall security policy ACL) ومراقبتها، وعلى تتبع الاستخدام من قبل مدير الشبكة (Administrator) |

## مرفق (5)
## محاور تدقيق المعلومات والتقنية المصاحبة له

| |
|---|
| مدى استخدام أجهزة IDS/ IPS على الشبكات، ومدى كفاية الإجراءات حيال عمليات المراجعة بشأنها، وفعّاليتها |
| مدى كفاية ضوابط الحماية المفعّلة 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 البنك المركزي العراقي بهذا الشأن |
| مدى كفاية إجراءات جرد الموجودات من أجهزة وبرامج ونظم المعلومات وفعّاليتها |
| مدى كفاية الإجراءات الخاصة وفعّاليتها، بحماية الأجهزة المختلفة من النفاذ غير المُصرَّح به، ومن الفيروسات، مثل النفاذ عبر الشبكات من خلال أجهزة كمبيوتر مجهزة بمنافذ (CD Rom,USB...etc) |
| مدى كفاية الإجراءات الخاصة بالحماية المادية لعناصر ومكوّنات الشبكات من النفاذ غير المُصرَّح به، مثل وجود (Open Ports) لعناصر الشبكات غير الفاعلة |
| مدى كفاية الإجراءات الخاصة بالحماية المادية لعناصر الشبكات (Switches,Routers,...etc) من الوصول غير المُصرَّح به |
| فحص متطلبات الأمن المادي والبيئي لغرف تشغيل مراكز البيانات والاتصالات الرئيسة والبديلة، بناءً على معايير تقييم مثل مدى ملاءمة الموقع، ودرجة حرارة ورطوبة مناسبة، وأرضية مرفوعة، ومكان وجود الغرفة في البداية، ووجود أجهزة إطفاء حريق آلي ونوعها (نوع الغاز المستخدم إذا كان مسموح باستخدامه بموجب المواصفة العراقية والعالمية)، وأجهزة إنذار وكشف الحريق وتسريب المياه، وكاميرات المراقبة والتسجيل، وسجل دخول الزوار، وحصر الدخول فقط للأشخاص المُصرَّح لهم، والضوابط المستخدمة في ذلك |
| مدى كفاية إجراءات المراجعة الدورية لملف الزوار للمؤسسة ولغرفة تشغيل مراكز البيانات والاتصالات |

# مرفق رقم (6)

## منظومة السياسات (حد أدنى)

| اسم السياسة | الغرض | النطاق |
|---|---|---|
| حوكمة تنظيم تقنية المعلومات والاتصالات | • وضع القواعد والمعايير اللازمة لإدارة موارد تقنية المعلومات والاتصالات، بما في ذلك الشكل الإداري (مركزي أو لامركزي)، والهياكل التنظيمية بما في ذلك النشاطات والمهام والمسؤوليات لإدارة تلك الموارد، بما في ذلك الموارد المالية. | عمليات وخدمات ومشاريع تقنية المعلومات والاتصالات |
| أمن المعلومات وحمايتها | • وضع القواعد والمعايير اللازمة لضمان متطلبات الحماية ، والسرية، والمصداقية، والتوافرية، والامتثال لإدارة موارد تقنية المعلومات والاتصالات بحسب المعايير الدولية المقبولة بهذا الشأن مثل (ISO-27001/2IEC). | جميع المعلومات والتقنية المصاحبة لها. |
| أمن بيانات بطاقات الدفع وحمايتها | اعتماد القواعد والمعايير اللازمة لضمان متطلبات الحماية، والسرية، والمصداقية، والتوافرية، والامتثال لإدارة أمن البيانات من قبل جميع الكيانات المشاركة في معالجة وإدارة بطاقات الدفع، بما في ذلك التجار، والمجهزين، والمؤسسات المالية، ومزودي خدمات الدفع الإلكتروني، فضلًا عن جميع الكيانات الأخرى التي تقوم بتخزين، ومعالجة، أو نقل بيانات حامل البطاقة و/ أو بيانات التصديق الحساسة بحسب المعايير الدولية المعتمدة بهذا الشأن واتخاذ جميع الإجراءات الفعلية للحصول على شهادة (PCI DSS) وفقًا لتلك المعايير. | بطاقات الدفع الإلكتروني |
| خطط استمرارية العمل وخطط التعافي من الكوارث | • وضع القواعد والمعايير اللازمة لبناء خطط التعافي من الكوارث وحماية الموظفين وخطط استمرارية الأعمال بما في ذلك آليات البناء والتشغيل والفحص والتدريب والتحديث على الخطط لضمان توافرية عمليات المؤسسة الحرجة | عمليات المؤسسة الحرجة؛ وحماية البشر. |
| إدارة مخاطر تقنية المعلومات والاتصالات | • وضع القواعد والمعايير اللازمة لبناء مخاطر تقنية المعلومات والاتصالات بوصفها جزءًا من المخاطر الكلية للمؤسسة، بما في ذلك حوكمة تلك المخاطر والمسؤوليات والمهام المناطة بالأطراف المختلفة، وآليات 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 والاتصالات (IT Compliance) | وضع القواعد والمعايير اللازمة لضمان الامتثال لضوابط البنك المركزي والجهات الرقابية الأخرى، وللقوانين والأنظمة السارية، ولسياسات المؤسسة. | جميع عمليات المؤسسة المعنية بموضوعات تقنية المعلومات والاتصالات. |

# مرفق رقم (6)

## منظومة السياسات (حد أدنى)

| اسم السياسة | الغرض | النطاق |
|---|---|---|
| خصوصية البيانات (Data Privacy) | وضع القواعد والمعايير اللازمة لحماية البيانات الخاصة بالأشخاص الطبيعيين أو المعنويين من عمليات الإفصاح والاستخدام غير المُصرَّح به. | البيانات الخاصة كافةً. |
| الاستعانة بخبرات خارجية (Outsourcing) | اعتماد سياسة عامة للاستعانة بالموارد بشكل عام وبموارد تقنية المعلومات والاتصالات بشكل خاص؛ تلك الموارد سواء المملوكة للمؤسسة (In-sourcing) أو المملوكة للغير (Outsourcing) تراعي الضوابط والأنظمة والقوانين وتحاكي أفضل الممارسات الدولية المقبولة بهذا الشأن؛ وتأخذ بالحسبان مكان العملية الإنتاجية ( On-site Near-site Off-shore Off-site)؛ وتاخذ بالحسبان وتراعي متطلبات مراقبة مستويات الخدمة (Service Levels) وتفعيل حق التدقيق (Audit Right) من قبل أطراف ثالثة محايدة موثوقة، وتحقيق متطلبات استمرارية العمل، وضوابط الحماية اللازمة لتلبية متطلبات السرية والمصداقية، فضلًا عن متطلبات الكفاءة والفعّالية في استغلال الموارد | عمليات المؤسسة كافةً |
| إدارة محفظة المشروع (Portfolio Management project) | وضع القواعد والمعايير اللازمة لإدارة المشاريع، بما في ذلك مراحل المشروع والحوكمة اللازمة لتحقيق المتطلبات المُتعلِّقة بالجودة (Quality Requirements)، وتلك المُتعلِّقة بالحماية والسرية (Confidentiality Requirements)، وتلك المُتعلِّقة بالامتثال تحقيقًا لأهداف المؤسسة وعملياتها. | جميع مشاريع المؤسسة المُتعلِّقة بتقنية المعلومات والاتصالات |

## مرفق رقم (6)

## منظومة السياسات (حد أدنى)

| | | |
|---|---|---|
| إدارة الموجودات ( Asset Management) | وضع القواعد والمعايير اللازمة لتصنيف درجة مخاطر البيانات والأنظمة المختلفة وتحديد مالكيها وضوابط حمايتها خلال مراحل دورة حياتها المختلفة. | البيانات والأجهزة والبرامج والأدوات المصاحبة لها. |
| الاستخدام المقبول لموارد تقنية المعلومات والاتصالات | وضع القواعد والمعايير اللازمة لتحديد السلوك المقبول وغير المقبول لموارد تقنية المعلومات والاتصالات. | الأجهزة والبرمجيات والتطبيقات والشبكات بما في ذلك الانترنت والبريد الإلكتروني |
| إدارة التغيير ( Change Management) | وضع القواعد والمعايير اللازمة لضمان مصداقية التغيير من حيث توثيق الموافقات اللازمة من مالكي الأصول الخاضعة للتغيير. | جميع عمليات تقنية المعلومات والاتصالات |
| أجهزة الحواسيب الرئيسة Servers | وضع قواعد ومعايير لتقليل عمليات النفاذ والاستخدام غير المشروع للأجهزة بما في ذلك ضوابط نفاذ موظفي دائرة تقنية المعلومات والاتصالات وذوي الامتيازات العليا لبيئات التشغيل، فضلًا عن معايير إدارة عمليات التشغيل اليومي للأجهزة والبرمجيات المختلفة بما في ذلك ضوابط الحماية وآليّات المراقبة والصيانة الدورية لتلك الأجهزة | جميع الحواسيب الرئيسة المملوكة أو المدارة من قبل المؤسسة لكل بيئات التطوير والفحص والتشغيل بما في ذلك نظم التشغيل والأدوات الأخرى المصاحبة لها. |
| أجهزة الكمبيوتر الطرفية | وضع قواعد ومعايير سلوكية وتقنية لضمان حماية البيانات الحسّاسة المُخزّنة على الأجهزة | كُلّ الأجهزة الطرفية المرتبطة بالشبكات أو القائمة بحد ذاتها |
| الأجهزة المحمولة | وضع قواعد ومعايير سلوكية وتقنية لضمان حماية البيانات الحسّاسة المُخزّنة على الأجهزة. | كُلّ الأجهزة المحمولة مثل (Smart، PDA، Laptop، Memory، USB، phone Cards.....Etc) |

# مرفق رقم (6)

## منظومة السياسات (حد أدنى)

| | | |
|---|---|---|
| إدارة صلاحيات وامتيازات النفاذ (User Access Management) | وضع قواعد ومعايير لضمان منح صلاحيات وامتيازات النفاذ للبيانات والبرامج والأجهزة لمستخدميها بحسب الحاجة للعمل وبالحد الأدنى بما يكفل السرية، والمصداقية، والتوافرية، لموارد تقنية المعلومات والاتصالات. | كُلّ البرامج والأجهزة وقواعد البيانات وما هو في حكمها. |
| تطوير/ اقتناء الأنظمة والبرمجيات ( system Development Life Cycle) | وضع القواعد والمعايير اللازمة لتنفيذ مراحل تطوير/ اقتناء الأنظمة والبرمجيات المختلفة لضمان تلبيتها لمتطلبات العمل من خلال منهجيات التطوير المختلفة المتناسبة مع متطلبات العمل وأهدافه. | كُلّ الاتفاقيات والتعاقدات والالتزامات مع الأطراف الخارجية والأطراف من داخل المؤسسة. |
| إدارة مستوى الخدمة Service Level (Management | وضع قواعد ومعايير لتحديد مستوى الخدمات المُقدَّمة، وقبولها، وتوثيقها، وقياسها، ومراقبتها، وتحسينها، سواء من أطراف داخلية أم أطراف خارجية لضمان الاستغلال الأمثل للموارد ودعم عمليات المؤسسة المختلفة. | كُلّ الاتفاقيات والتعاقدات والالتزامات مع الأطراف الخارجية والأطراف من داخل المؤسسة. |
| النسخ الاحتياطي والاسترجاع (Back-up and Restore) | وضع قواعد ومعايير لآليات النسخ الاحتياطي والاسترجاع لضمان توافرية البيانات ومصداقيتها وسريتها. | البيانات في بيئات التشغيل وحيثما يلزم. |
| الاحتفاظ بالبيانات (Data Retention) | وضع قواعد ومعايير الخاصة بحجم البيانات الواجب توافرها سواء بشكل ورقي أو تلك المتواجدة على أجهزة الحواسيب والتطبيقات المختلفة والمدة الزمنية الواجب الاحتفاظ بها والمفاضلة بين حجم البيانات المتوافرة وسرعة الأداء في الوصول إلى البيانات. | كُلّ الأجهزة والبرمجيات ووسائل وأدوات الاحتفاظ بالبيانات. |
| شراء الأنظمة والتجهيزات (Purchasing Systems) | وضع قواعد ومعايير للمفاضلة بين المزوِّدين الخارجين. | كُلّ التجهيزات التقنية والبرامج المُتعلِّقة بها. |

## مرفق رقم (6)

## منظومة السياسات (حد أدنى)

| | | |
|---|---|---|
| النفاذ عن بعد (Remote Access) | وضع قواعد ومعايير للربط الشبكي عن بعد بشبكات الحواسيب الخاصة بالمؤسسة لتقليل مخاطر الاطلاع والاستخدام لبيانات ومصادر المؤسسة الحساسة ولأنظمة الضبط والرقابة الداخلية المعنية بحماية موجودات المؤسسة؛ وللحماية من مخاطر السمعة. | الأطراف والشركاء الدخليين والخارجيين مثل مزوّدي الخدمات؛ ولجميع بيئات التطوير والفحص والتشغيل للأجهزة والشبكات؛ ومنها على سبيل المثال لا الحصر شبكات الانترنت، والشبكات المُشفَّرة، وخطوط الاتصال المختلفة مثل (ISDB، Frame relay VPN DSL MPLS) |
| الشبكات (Networks) | وضع قواعد ومعايير لضمان تحقيق متطلبات الكفاءة والفعّالية فى استغلال عناصر الشبكات والإتصالات من جهة وتحقيق متطلبات الأمن والحماية من جهة أخرى دعمًا لتحقيق أهداف المؤسسة. | كُلّ عناصر الشبكات بجميع البيئات |
| الشبكات اللاسكلية (Wireless Networks) | وضع قواعد ومعايير بغرض حماية البيانات الحساسة المتناقلة عبر الشبكات اللاسكلية من الاعتراض والاستخدام غير المشروع. | كُلّ الشبكات اللاسكلية الفعلية منها والافتراضية |
| الجدران النارية (Firewalls) | وضع الحدّ الأدنى من القواعد والمعايير المنظمة لآلية عمل أجهزة الجدران النارية، وآلية حمايتها (Firewalls) لتفعيلها بالشكل المطلوب والكفيل بحماية وضمان سرية ومصداقية بيانات وعمليات المؤسسة وتوافريتها. | كُلّ أجهزة الـ(Firewalls) العاملة بالبيئات كافّةً، مثل (External، proxy، DNS DNS VPN Routers Switches servers...etc). |
| فحص الاختراق وتحليل الثغرات (penetrating Testing and Vulnerability Assessment) | وضع قواعد ومعايير لفحص الأجهزة وعناصر الشبكات لضمان عدم وجود ثغرات أمنية تُمكّن من اختراق البيانات والأنظمة والعمليات الحساسة للمؤسسة. | كُلّ موجودات المؤسسة التقنية من أجهزة حواسيب رئيسة وحماية عناصر الشبكات والبرمجيات. |
| مقسّم الهاتف الخاص (Pravit Branch Exchange) | وضع الحد الأدنى من قواعد ومعايير الحماية لأنظمة المُقسّم لضمان الحماية والسرية لبيانات وعمليات المؤسسة من الاستخدام غير المشروع | كُلّ أجهزة المُقسّم المملوكة وغير المملوكة للمؤسسة |

## مرفق رقم (7)

## المعلومات والتقارير (حد أدنى)

| اسم التقرير | محتوياته |
|---|---|
| مصفوفة الصلاحيات والامتيازات (Authority Matrix) | مصفوفة تُحدِّد الصلاحيات والامتيازات الممنوحة على جميع البرامج وقواعد البيانات وعناصر الشبكات؛ مثل التفاصيل اسم المستخدم ووظيفته وصلاحياته أو امتيازته |
| تحليل عوامل مخاطر تقنية المعلومات والاتصالات (IT Risk Factors Analysis) | 1- التهديدات الداخلية.<br>2- التهديدات الخارجية.<br>3- مواطن الضعف في إدارة موارد تقنية المعلومات والاتصالات.<br>4- مواطن الضعف في قدرة تقنية المعلومات والاتصالات على تمكين عمليات المؤسسة.<br>5- مواطن الضعف في إدارة مخاطر تقنية المعلومات والاتصالات. |
| تحليل سيناريو مخاطر تقنية المعلومات والاتصالات (IT Risk Scenario Analysis) | 1- مصدر التهديد إمّا داخلي أو خارجي<br>2- نوع التهديد (Threat Type) مثل الأخطاء، أو اختراق فيروس، أو أحداث خارجية.<br>3- الحادث(Event): مثل الإفصاح عن معلومات سرية، أو تعطل؛ أو تعديل غير مشروع؛ أو سرقة وتدمير؛ أو تصميم غير فعّال للقوانين والأنظمة؛ أو الاستخدام غير المقبول.<br>4- الأصول المتأثرة (Asset or Resource Affected): مثل بشر؛ أو هياكل تنظيمة لعمليات البنية التحتية لتقنية معلومات؛ أو معلومات برامج.<br>5- الوقت : وقت الحدوث، مدة الحادث عمر الحادث قبل اكتشافه. |
| سجل مخاطر تقنية المعلومات والاتصالات (IT Risk Register) | 1- مُقدّمة: مالك الأصل، فريق التقييم، تاريخ التقييم اللاحق، مُلخّص تقييم المخاطر، وخيار إدارة المخاطر.<br>2- سيناريو تحليل مخاطر تقنية المعلومات والاتصالات في أعلاه.<br>3- تقييم مخاطر تقنية المعلومات والاتصالات من حيث احتساب محوري المخاطر متمثلة باحتمالية الحادث (potentiality)، وحجم الأثر (Impact or Severity)، وبفضل استخدام مقياس معياري زوجي لمحاور التقييم، وإظهار حجم الأثر استنادًا إلى أهداف وعمليات المؤسسة المتضمنة تقنية المعلومات والاتصالات باستخدام محاور التقييم لأحد النماذج العالية الآتية على سبيل المثال:<br>أ. COBIT Information Criteria<br>ب. COBIT for Risk<br>ت. Balanced Scorecard(BSC)<br>ج. Extended BSC<br>د. Westerman<br>ه. COSO ERM<br>و. FAIR (Factor Analysis of Information Risk)<br>4 - قابلية تحمُّل المخاطر (Risk Appetite)<br>5- خيار إدارة المخاطر (مقبول (في حال كانت كمية المخاطر المحسوبة أقل من قابلية تحمُّل المخاطر)، تخفيف، تجنُّب، تحويل).<br>6- بنود خطة إدارة المخاطر ومتابعتها (نُفِّذت، أو قيد التنفيذ بحسب الخطة)<br>7- معايير أداء رئيسة لمراقبة مستوى المخاطر (Key Risk Indicators) للتأكد من عدم تجاوز قابلية تحمُّل المخاطر ودرجة تحمُّل المخاطر (نسبة الانحراف الموجب للقابلية تحمُّل المخاطر). |

## مرفق رقم (7)

## المعلومات والتقارير (حد أدنى)

| | |
|---|---|
| RACI Chart | قوائم تتضمن تحديد الجهة أو الجهات أو الشخص أو الأطراف المسؤولة بشكل أولي (Responsible) وتلك المسؤولة بشكل نهائي (Accountable)، وتلك المستشارة (Consulted)، وتلك التي يتمّ إطلاعها (Informed) لكل عمليات إدارة موارد تقنية المعلومات والاتصالات؛ وإدارة مخاطر وأمن المعلومات والرقابة مستقلة. |
| ملف المخاطر (IT Risk Profile) | 1- سجل المخاطر.<br>2- تحليل عوامل المخاطر.<br>3- الخسائر المتحققة وغير المحققة (Losses and Near-Misses)<br>4- تدقيق جهات مستقلة. |
| تقارير المخاطر (IT Risk Report) | يوضح كمية مخاطر تقنية المعلومات والاتصالات الحالية المتضمنة في عمليات المؤسسة؛ والإجراءات المتخذة أو التي سيتم اتخاذها لإدارة تلك المخاطر؛ ويتمُّ تصميم شكل وطريقة عرض هذه التقارير بحيث تخدم متّخذ القرار مالك العملية/ العمليات التي تقع ضمن مسؤوليته بحسب طلبه. |
| خريطة المخاطر (IT Risk Map or Heat map) | رسم بياني يوضح محورَي المخاطر (الاحتمالية والأثر) ومناطق المخاطر المقبولة وغير المقبولة بحسب قابلية تحمّل المخاطر بموجب ألوان تساعد على توضيح ذلك، وتوشر عليه مخاطر تقنية المعلومات والاتصالات المحسوبة والموجودة في عمليات ذلك. |
| Risk Universe Appetite and Tolerance | تقرير يوضح جميع المخاطر المتضمنة في العملية بما فيها مخاطر تقنية المعلومات والاتصالات، يوضح كمية المخاطر المخطط قبولها (Risk Appetite) ونسبة الانحراف الموجب على قابلية تحمّل المخاطر (Risk Tolerance). |
| مؤشرات قياس المخاطر الرئيسة (key Risk Indicators) | عبارة عن معايير قياس يتمّ تحديدها ومقارنتها بـ(Benchmark) لمراقبة المخاطر الحالية للتأكد من عدم تجاوزها للقابلية على تحمّل المخاطر، ويتمّ تحديدها لتكون موشرات قياس رئيسة استنادًا إلى المعايير الآتية:<br>أ- الأثر: حصة وحجم الموشر في قياس أثر المخاطر.<br>ب- القابلية للقياس.<br>ج- الاعتمادية.<br>د- الحسّاسية. |
| Risk Taxonomy | توضح معاني المصطلحات المستخدمة في تعريف وقياس وإدارة ومراقبة المخاطر، فضلًا عن معايير قياس المخاطر والتعبير عنها، بحيث يتمّ استخدام تلك المصطلحات بالمعنى والمفهوم ذاتيهما لدى جميع الشركاء، وبما يتفق وضوابطنا بهذا الشأن. |
| Risk and Control Activity Matrix(RCAM) | مصفوفة تُبيّن كمية المخاطر المحسوبة والإجراءات والضوابط المقابلة المتخذة لإدارة تلك المخاطر ومدى كفايتها، والسيطرة عليها. |

## مرفق رقم (7)

## المعلومات والتقارير (حد أدنى)

| | |
|---|---|
| موازنة أمن المعلومات وحمايتها | يتمُّ تحديد المصاريف المُخطّط لإنفاقها على أمن المعلومات للعام القادم ضمن الموازنة العامة للمؤسسة وبما يتوافق والمشاريع المُخطَّط لتنفيذها، متضمنة تحليل الانحراف القائم لمصاريف العام الحالي مقارنة مع الموازنة المُحدَّدة للعام نفسه. |
| MIS Report | مصفوفة تبيّن جميع أنواع التقارير المنتجة بحيث تظهر اسم مالك التقرير، ووظيفته، ودورية إنتاجه، والإجراء المتخذ تجاهه. |
| استراتيجية أو منهجية تدقيق تقنية المعلومات والاتصالات (Audit Strategy) | يتمُّ تحديد أهداف تدقيق تقنية المعلومات والاتصالات ونطاق التدقيق وبرامج التدقيق المستخدمة في عمليات المراجعة. |
| ميثاق تدقيق تقنية المعلومات والاتصالات (IT Audit charter) (Engagement Letter) | ميثاق مستقل أو ضمن الميثاق العام للتدقيق الداخلي يتمُّ فيه تحديد صلاحيات عمل تدقيق تقنية المعلومات والاتصالات، ومسؤولياته، وطبيعته، ونطاقه، وبما يتفق وضوابطنا بهذا الشأن ويتمُّ تضمين الـ(Engagement Letter) الموقّعة مع المُدقِّق الخارجي بذلك أيضًا. |
| خطة تدقيق تقنية المعلومات والاتصالات (IT Audit plan) | يتمُّ رسم خطة مستقبلية للتدقيق تكون مرتكزة ومبنية على المخاطر. |
| مصفوفة المؤهّلات (HR Competencies) | تتضمن الشهادات الأكاديمية والمهنية والفنية ومجموع الخبرات والمهارات اللازم امتلاكها لكوادر إدارة تقنية المعلومات والاتصالات ،وإدارة مخاطر تقنية المعلومات والاتصالات، والتشغيل، وتدقيق تقنية المعلومات والاتصالات، وأمن المعلومات وحمايتها. |
| سجل تدقيق تقنية المعلومات والاتصالات (Assurance Findings Register) | يحتوي جميع نقط وملحوظات التدقيق والإجراءات والمتابعات المتخذة حيالها. |
| ملف تدقيق تقنية المعلومات والاتصالات (Assurance Report Repository) | يحتوي كُلّ تقارير تدقيق تقنية المعلومات والاتصالات |
| افضل المعايير الدولية لإدارة موارد ومشاريع تقنية المعلومات والاتصالات وإدارة مخاطر تقنية المعلومات والاتصالات وأمن وحماية والتدقيق على تقنية المعلومات والاتصالات | يتمُّ إنشاء مكتبة بالمراجع المطلوبة بحسب أفضل الممارسات الدولية وتوفير استخدامها لكادر المؤسسة بحسب طبيعة العمل، فضلًا عن منظومة القوانين والأنظمة والضوابط المراعاة. |

## مرفق رقم (8)
## الخدمات والبرامج والبنية التحتية لتقنية المعلومات والاتصالات

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

## مرفق رقم (8)
## الخدمات والبرامج والبنية التحتية لتقنية المعلومات والاتصالات

| اسم الخدمة، البرنامج، الأداء | وصف |
|---|---|
| أمن وحماية البيانات والمعلومات المنطقي | مجموع الأفراد والإجراءات والبرامج والأداوات المستخدمة في الحفاظ على سرية البيانات والمعلومات، ومصداقيتها وتوافريتها، واستخدام أداوت، مثل:<br>• PKI sniffers DPI<br>• Encryption services<br>• Firewalls<br>• Packet analyzer sensors<br>• IPS \IDS<br>• Data loss prevention (DLP)<br>• System and device management solutions<br>• Software distribution solutions<br>• Remote management systems<br>• Virtualization and cloud management solutions<br>• Document management<br>• Data classification systems<br>• Application-centric data management solutions<br>• Data obfuscation solutions<br>• Vendor information security advisories and KBs<br>• Honeypots tarpits<br>• Antimalware antirootkit antispyware antiphishing |
| مراقبة أمن المعلومات | مجموع الأفراد والإجراءات والبرامج والأدوات المستخدمة لضمان توفير وسائل المراقبة المستمرة لتحقيق أهداف أمن المعلومات وحمايتها، مثل:<br>• Logs<br>• SNMP<br>• Alternting system<br>• SIEM (Security Information and Event Management)<br>• Management dashboards<br>• Network operations centers (NOCs) |
| برمجيات تدقيق تقنية المعلومات والاتصالات | البرمجيات المساعدة في تدقيق تقنية المعلومات والاتصالات وكشف الاحتيال، والبرمجيات المستخدمة في التخطيط، وتقييم المخاطر، وكتابة تقارير التحقيق، وتوثيقها، والنفاذ إليها. مثل:<br>• CAATs (Computer Assisted Audit Techniques)<br>• Document management systems<br>• Planning tool<br>• Tracking issues system<br>• Data analytics/sampling techniques<br>• Workflow systems |

## مرفق رقم (8)
## الخدمات والبرامج والبنية التحتية لتقنية المعلومات والاتصالات

| اسم الخدمة، البرنامج، الأداء | وصف |
|---|---|
| الاستضافة وضوابط الأمن المادي والبيئي لغرف الخوادم الرئيسة وغرف الاتصالات والتزوّد بالكهرباء | توفير ضوابط الأمن المادي والبيئي بالحد الأدنى بحسب ما يأتي:<br>• يُراعَى تواجد الغرف وأن تكون البنية التحتية للبناية بعيدة في تصميمها، ومحمية عن تهديدات فيضانات وتسربات المياه والصرف الصحي المحتملة، سواء أسفل البناء، أو في نهايته بالقرب من الأسطح، أو أي مكان آخر مُعرَّض لذلك. ويجب أن تكون مساحة الغرف كافية وتلبي احتياجات المؤسسة الحالية وتأخذ بالحسبان التوسع المستقبلي المحتمل<br>• يجب أن يكون مكان الغرف والبناية بشكل عام غير محدود الوصول (سواء في طبيعة الموقع الجغرافي، أم بموجب الاتفاقيات التعاقدية الحصرية) من قبل شركات الاتصالات كافّةً ومن مزوّدين متنوعين<br>• يجب أن تتمتع غرف الخوادم الرئيسة وغرف الاتصالات (مثل: Routers, switches,...etc) غرف تزويد الكهرباء بالحماية المادية والبيئية بحيث تكون محاطة بجدران مسلحة من دون شبابيك، ومعزولة من حيث التأثيرات الكهرومغناطيسية التي تؤثّر سلبًا في بيانات أجهزة الكمبيوتر، ومخدومة بمدخل احتياطي محكم لاستخدامه من قبل الأفراد عند الطوارئ، ويجب أن تكون الغرفة من حيث التصميم مخدومة بمداخل الكهرباء وأجهزة مكافحة الحريق، ويجب أن تحتوي على كواشف للدخان، والمياه، والحرارة، والرطوبة، بدرجة حماية عالية، ويجب أيضًا توفير المراقبة التلفزيونية المسجّلة، والتبريد المُوزَّع على جميع مساحة الغرفة بشكل عادل؛ لحماية الأجهزة من الحرارة والرطوبة المرتفعة، مع توفير أجهزة لسحب الغبار من الغرفة، وأن يكون الدخول محكمًا ومراقبًا بحيث يُمنَع غير المُخوَّلين من ذلك، مع مراعاة عدم وضع أيّة إشارات تدلّ الغير على مكان تواجد تلك الغرف الحسّاسة في المؤسسة من دون مرافقين مُخوَّلين.<br>• يجب تزويد غرف الخوادم وغرف الاتصالات بمداخل كهرباء متعدّدة المصادر وأن يكون التحويل بينها بشكل أوتوماتيكي، أي: توفير بطاريات (UPS)، فضلًا عن مولدات كهرباء بالقدرة الكافية لتشغيل أجهزة وعمليات المؤسسة (الحسّاسة في الأقل)، في حال انقطاع مصدر الكهرباء الرئيس.<br>• يجب الأخذ بالحسبان متطلبات الدفاع المدني ودائرة المواصفات والمقاييس (حيثما تطلب الأمر ذلك).<br>• كل ما ذُكِرَ آنفًا، ينطبق أيضًا على غرف الخوادم والاتصالات والكهرباء البديلة (Disaster Recovery Sites). |

## مرفق رقم (8)
## الخدمات والبرامج والبنية التحتية لتقنية المعلومات والاتصالات

| اسم الخدمة، البرنامج، الأداء | وصف |
|---|---|
| المعايير والمواصفات القياسية العالمية المعتمدة في إنشاء مراكز البيانات (CENTER DATA) | • Uptime institute, TUI Tier Standard: Operational Sustainability<br>• ANSI/TIA-942-A Infrastructure Standard for Data Centers<br>• ANSI/BICSI 002 Data Center Design and Implementation Best Practices<br>• CENELEC EN 50600 Information technology — Data centre facilities and infrastructures<br>• CENELEC EN 50173-5 Information Technology - Generic Cabling Systems<br>• ISO/IEC 24764 Information technology - Generic Cabling Systems for Data Centres<br>• ASHRAE 90.4-2016 - Environmental Conditions<br>• ISO 9000 - Quality System<br>• ISO14000 - Environmental Management System<br>• IS0 27001 - Information Security<br>• PCI – Payment Card Industry security standard<br>• AMS-IX - Amsterdam Internet Exchange, Data Centre business continuity standard |