بسم الله الرحمن الرحيم

الرقـــم: ١/١٧/ ١٤٦٩٣
التاريـــخ: ٢٠/صفر/ ١٤٤٣هـ
الموافـــق: ٢٠٢١/٠٩/٢٧ م

السادة شركات التأمين المحترمين

تحية طيبة وبعد،

بالإشارة إلى تعميم رقم (٢٠١٩/٣٣/٢١٤٤) بتاريخ ٢٠١٩/٠٧/٢١ حول معيار التقارير المالية الدولي رقم (١٧)، نرفق لكم الدليل الإرشادي لتطبيق متطلبات معيار التقارير المالية الدولي رقم (١٧) والذي يحدد الحد الأدنى من الجوانب الواجب مراعاتها عند إعداد السياسات والإجراءات واتخاذ القرارات المرتبطة بمتطلبات المعيار.

وتفضلوا بقبول فائق الاحترام.

البنك المركزي الأردني

نسخة الاتحاد الأردني لشركات التأمين.

دليل إرشادات تطبيق متطلبات معيار التقارير المالية الدولي رقم (١٧)

٢٠٢١

الموضوع	المحتويات	الصفحة

المقدمة

أصدر مجلس معايير المحاسبة الدولية في شهر مايو من عام ٢٠١٧ معياراً جديد يتعلق بعقود التأمين والذي كان من المقرر بدء تطبيقه اعتبارا من ٢٠٢١/١/١ والذي سيحل محل معيار التقارير المالية الدولي (٤) المطبق حالياً، وفي اجتماعه المنعقد بتاريخ ٢٠١٨/١١/١٤ وافق مجلس معايير المحاسبة الدولية على تأجيل تطبيق المعيار لمدة سنة َاضافية تبدأ ٢٠٢٢/١/١ وطرح الموضوع للمناقشة العامة. وتم لاحقاً في تاريخ ٢٠٢٠/٣ التصويت على تأجيل تطبيق متطلبات المعيار حتى تاريخ ٢٠٢٣/١/١.

يمثل معيار التقارير المالية الدولي رقم (١٧) مراجعة شاملة للحسابات المتعلقة بعقود التأمين، الذي من شأنه تعزيز شفافية الأداء المالي الفعلي لشركات التأمين، ويهدف إلى أن تكون البيانات المالية للشركات أكثر دقة في قياس النتائج والاعتراف بالإيرادات والالتزامات وأن تكون أكثر قابلية للمقارنة مع شركات التأمين الأخرى.

يعالج المعيار النواحي المحاسبية للعقود التي تصدرها شركات التأمين، ويختلف أثر هذا المعيار بحسب نوعية العقود التي تكتتبها كل شركة، حيث سيكون الأثر الأكبر على عقود التأمين طويلة الأجل، ومع ذلك، سيكون التغيير جوهري لجميع شركات التأمين.

سيؤدي تطبيق المتطلبات الواردة في المعيار الجديد إلى إحداث تغييرات في عمليات شركات التأمين، مما يتطلب من شركات التأمين تغيير طرق المعالجة المحاسبية لعقود التأمين وآلية إعداد وعرض التقارير المالية وحاجة شركات التأمين إلى تعديل وتطوير الأنظمة وإعادة هيكلة عملياتها التشغيلية، حيث تضمنت إجراءات عمل مجلس معايير المحاسبة الدولية (IASB)، مبادئ جديدة للاعتراف بالخسائر المتوقعة واتباع منهج محدد لمحاسبة عقود التامين، الأمر الذي يتطلب من شركات التأمين إعداد سياسات وإجراءات وقرارات تضمن قدرة الشركة على تطبيق متطلبات المعيار بالشكل الأمثل.

يراعي معيار التقارير المالية الدولي رقم (١٧) القيمة الزمنية للنقود عند قياس التزامات عقود التأمين بحيث تظهر بالقيمة الحالية لتدفقات النقدية المستقبلية باستخدام معدل خصم يعكس المخاطر التي تتعرض لها الشركة، على أن يتم مراجعتها وتحديثها بشكل دوري.

تم إعداد هذا الدليل الإرشادي لمساعدة شركات التأمين في تطبيق متطلبات معيار التقارير المالية الدولي رقم (١٧) مع مراعاة تعقيد وخصوصية عمليات شركات التأمين المختلفة، إضافة الى زيادة مستوى الشفافية وضمان عرض بيانات مالية ملائمة وموضوعية، حيث يتناول هذا الدليل الآليات والإجراءات الواجب اتباعها من قبل مجالس ادارة شركات التأمين العاملة في القطاع بهدف تطبيق المعيار، بالإضافة الى توضيح لمتطلبات أنظمة تقنية المعلومات وأمن المعلومات ومتطلبات تطبيق هذا المعيار وتأثيره المباشر على العمليات الإدارية، وذلك من منطلق اهتمام البنك المركزي بضمان قيام شركات التأمين بتطبيق المعيار بالشكل الأمثل، وبذلك يجب على شركات التأمين مراعاة الحد الأدنى من المتطلبات المذكورة في الدليل.

الفصل الأول
متطلبات تطبيق معيار التقارير المالية الدولي رقم (١٧)

أولا: تعريف العقد

- على الشـــركة إعداد ســـياســـة معتمدة من مجلس الإدارة تمكنها من تحديد إذا ما كان العقد ينطبق عليه تعريف عقد تأمين الوارد في المعيار.
- تتضمن السياسة المشار إليها أعلاه بالحد الأدنى ما يلي:
  - تعريف عقد التأمين
  - تحديد العقود التي تصدرها الشركة التي تنسجم مع تعريف عقد التأمين.
  - تحديد العقود التي تصدرها الشركة والتي لا تنسجم مع تعريف عقد التأمين
  - تعريف المخاطر التأمينية الجوهرية.
  - آلية تحديد الأهمية النسبية لمخاطر عقد التأمين.

ثانياً: فصل مكونات عقد التأمين

- على الشـركة دراسـة العقود التي تكتتب بها والتأكد من عدم وجود مكونات في تلك العقود لا تنسـجم مع المعيار، وفي حال وجودها على الشركة التأكد من إمكانية فصل تلك المكونات ومعالجتها حسب المعيار الأكثر اختصاصا وفق سياسة لفصل مكونات عقد التأمين معتمدة من مجلس الإدارة.
- تتضمن السياسة المشار إليها أعلاه بالحد الأدنى ما يلي:
  - آلية فصل المكونات غير التأمينية عن عقد التأمين.
  - آلية تحديد الضمانات المدمجة وكيفية معالجتها -ان وجدت-
  - المعيار الأكثر اختصاصا الذي سيتم تطبيقه لمعالجة المكونات غير التأمينية.
  - آلية تحديد الأهمية النسبية لمكونات عقد التأمين.

ثالثاً: مستوى التجميع

- على الشركة إعداد سياسة معتمدة من قبل مجلس الإدارة لتجميع عقود التأمين ضمن محافظ منفصلة يتم تبويبها ومعالجتها بشكل مستقل على أن تقسم إلى ثلاثة مستويات على التوالي كما يلي:

١) المخاطر المتشابهة والتي تدار معاً.
٢) سنة الاكتتاب.
٣) الربحية.

- المستوى الأول (المخاطر المتشابهة)

يجب على شركات التأمين أن تقوم بتجميع محافظ عقود التأمين حسب تشابه مخاطر تلك العقود وعلى أن تكون بالحد الأدنى كما يلي:

- محفظة تامين المركبات الإلزامي.
- محفظة تأمين المركبات الشامل.
- محفظة تأمين مجمع الحافلات.
- محفظة التأمين الهندسي.
- محافظ التأمين الخاصة بالعطاءات التي تمتد لأكثر من سنة.
- محافظ عقود التأمين الأخرى حسب تقديرات وخبرة الشركة.

- المستوى الثاني (سنة الاكتتاب)

على الشركة تصنيف محافظ عقود التأمين وفق التصنيفات المشار إليها في المستوى الأول إلى مجموعات حسب سنة الاكتتاب مثال (جميع العقود التي تم إصدارها خلال سنة ٢٠٢٠ تعالج بشكل في مجموعة مستقلة عن العقود المصدرة في ٢٠٢١ وهكذا).

- المستوى الثالث (الربحية)

على الشركة تصنيف مجموعات العقود المشار إليها في المستوى الثاني إلى التصنيفات المبينة أدناه، وذلك حسب صافي التدفقات النقدية المتوقعة من العقد والمنهج المحاسبي المتبع في معالجة مجموعات العقود كما سيتم الإشارة إليه لاحقا في هذا الدليل:

- العقود التي لا توجد احتمالية أن تصبح مثقلة بالأعباء عند الاعتراف الأولي.
- العقود المثقلة بالأعباء.
- العقود أخرى -إن وجدت-.

رابعاً: الاعتراف بالعقود وتعديلاتها

- على الشركة الاعتراف بمجموعة عقود التأمين اعتبارا من التواريخ التالية أيهما أسبق:
  - بداية فترة التغطية.
  - استحقاق أول دفعة.
  - عندما تصبح مجموعة العقود مثقلة بالأعباء.
- فيما يخص التعديلات التي قد تطرأ على العقود، على الشركة إعداد سياسة معتمدة من قبل مجلس الإدارة، بحيث تتضمن بحد أدنى ما يلي:
  - تعديلات العقد التي تعتبر "هامة"، وآلية معالجة تلك التعديلات.
  - الحالات التي يتم إلغاء الاعتراف بالعقد والآلية المستخدمة في معالجته.

خامساً: التدفقات النقدية المستقبلية

- تعرّف التدفقات على انها جميع المبالغ المتوقع تحصيلها والمتوقع دفعها الناتجة عن عقود التأمين، ويجب تقديرها عند الاعتراف بعقد التأمين بناءً على سياسة معتمدة من قبل مجلس الإدارة تتضمن فرضيات اكتوارية وخبرة الشركة في إدارة مجموعة عقود التأمين، حيث تتضمن التدفقات النقدية المستقبلية بالحد الأدنى ما يلي:

١) التدفقات النقدية المستقبلية المتوقع تحصيلها (Cash Inflow)
- الأقساط المكتتبة، مع مراعاة آلية دفع تلك الأقساط المحددة في عقد التأمين.
- الايرادات المرتبطة بعقد التأمين مثل رسوم اصدار عقود التأمين.
- الإيرادات الناتجة عن المستردات المتوقعة والحطام.

٢) التدفقات النقدية المستقبلية المتوقع دفعها (Cash Outflow)
- التقدير الأفضل لتكلفة المطالبات المتكبدة، والمطالبات التي حدثت ولم يتم التبليغ عنها.
- المطالبات المتوقع تكبدها، بما فيها المدفوعات الناتجة عن المكونات الغير تأمينية التي لا يمكن فصلها.
- المصاريف الإدارية ونفقات الموظفين المرتبطة بعقود التأمين.
- تخصيص التدفقات النقدية الخاصة بتكاليف الاستحواذ.
- التكاليف المتكبدة في تقديم خدمات غير مالية (صيانة المركبات، إعادة بناء المنزل).
- تكاليف معالجة المطالبات (معاين خسائر، مصاريف قضائية).

٣) التدفقات النقدية المستقبلية التي يجب استثناؤها عند احتساب ربحية عقد التأمين:
- التدفقات النقدية التي تنشأ بموجب عقود إعادة التأمين المحتفظ بها مثل العمولات المقبوضة وفوائد مدفوعة على الأرصدة المحتجزة.
- عوائد الاستثمار.
- التدفقات النقدية التي قد تنشأ من عقود التأمين المستقبلية.
- التدفقات النقدية الناشئة عن المكونات المنفصلة عن عقد التأمين.
- التدفقات النقدية التي لا ترتبط بمحفظة عقود التأمين.

- على الشركة مراعاة الجوانب المبينة أدناه عند وضع الفرضيات المتعلقة بعملية تقدير التدفقات النقدية المستقبلية لمجموعات عقود التأمين:
  - المخاطر المتأصلة.
  - مستوى التجميع.
  - احتمالية حدوث كوارث طبيعية.
  - احتمالية تصفية العقد قبل تاريخ انتهاء التغطية التأمينية، وغيرها من الممارسات المتوقعة من حامل عقد التأمين.
  - العوامل التي ستؤثر على التقديرات، ومصادر المعلومات لهذه العوامل.

سادساً: تكاليف الاستحواذ

- على الشركة إعداد سياسة معتمدة من قبل مجلس الإدارة ويتم تقييمها من قبل الخبير الإكتواري المعين من قبل الشركة تمكنها من تخصيص تكاليف الاستحواذ حسب مجموعة عقود التأمين، وطريقة معالجتها، بحيث تتضمن بحد أدنى ما يلي:
  - آلية تقدير تكاليف الاستحواذ عند إعداد الموازنات التقديرية.
  - آلية إطفاء تكاليف الاستحواذ.
- تلتزم شركة التأمين بتأجيل الاعتراف بتكاليف الاستحواذ، على أن يتم اثبات تكاليف الاستحواذ المؤجلة في بيان المركز المالي، واطفائها وفق الآلية المعتمدة في السياسة المشار إليها اعلاه.

سابعاً: معدل الخصم

- على الشركة إعداد سياسة معتمدة من قبل مجلس الإدارة لتحديد معدل الخصم ويتم تقييمها من قبل الخبير الإكتواري المعين من الشركة، على أن تتضمن بالحد الأدنى ما يلي:
  - تحديد الآلية المتبعة في احتساب معدل الخصم.
  - آلية مراجعة الفرضيات المستخدمة في احتساب معدل الخصم.
  - أن يكون معدل الخصم متسق مع أسعار السوق، ويعكس القيمة الزمنية للنقود وخصائص التدفقات النقدية وخصائص السيولة في عقود التأمين.
  - يجب أن يكون معدل الخصم متوافق مع العُملة التي تم تسجيل التزامات العقود بها.
  - تحديد منحنى العائد المستخدم في خصم التدفقات النقدية في حال استخدام أحد الطرق التي تعتمد على منحنى العائد.
  - آلية معالجة مصروف/ ايراد التمويل.
- يتم تطبيق معدل الخصم على التدفقات النقدية عند احتساب البنود التالية:
  - الالتزامات مقابل المطالبات المتكبدة (المطالبات المتوقع سدادها خلال أكثر من ١٢ شهر).
  - الالتزامات مقابل التغطية المتبقية (المنهج العام/ التكلفة المتغيرة).

ثامناً: تعديلات المخاطر غير المالية

- على الشركة إعداد سياسة معتمدة من قبل مجلس الإدارة لاحتساب تعديلات المخاطر غير المالية لكل مجموعة عقود التأمين كجزء من سياسة إدارة المخاطر يتم تقييمها من قبل الخبير الإكتواري المعين من الشركة، بحيث تتضمن تلك السياسية بالحد الأدنى ما يلي:
  - تعريف المخاطر غير المالية مثل مخاطر الزيادة في قيمة المطالبات والمصروفات، باستثناء المخاطر المرتبطة بمؤشر التضخم، حيث تعتبر هذه مخاطر مالية.
  - تحديد الطريقة التي سيتم اتباعها في رصد قيمة تعديلات المخاطر غير المالية.
  - مستوى الثقة المستخدم لاحتساب قيمة تعديلات المخاطر غير المالية.

- على الشركة تضمين قيمة تعديلات المخاطر غير المالية بشكل صريح عند احتساب البنود التالية:
  - الالتزامات المتعلقة بالمطالبات المتكبدة.
  - الالتزامات مقابل التغطية المتبقية (المنهج العام/ التكلفة المتغيرة).

تاسعاً: مناهج قياس العقود

- أتاح المعيار لشركات التأمين ثلاثة مناهج لقياس ومعالجة عقود التأمين وعقود إعادة التأمين المحتفظ بها محاسبياً، وهي كالتالي:

١) منهج تخصيص الأقساط (Premium Allocation Approach)

يطبق على مجموعات عقود التأمين المبينة أدناه:

- التي لا تتجاوز مدة التغطية التأمينية سنة واحدة.
- التي يكون فيها قيمة "الالتزامات مقابل التغطية المتبقية" لا تختلف عن قيمته عند تطبيق متطلبات المنهج العام بشكل جوهري.

مع مراعاة وجوب استخدام معدل خصم لاحتساب القيمة الحالية للتدفقات النقدية في حال تم تطبيق المنهج على مجموعة عقود مدة تغطيتها تزيد عن سنة وفقاً للاستثناء المذكور سابقاً.

٢) المنهج العام (General Measurement Model)

يطبق على جميع عقود التأمين حيث يتطلب قياس التزامات مجموعات عقود التأمين عن طريق خصم التدفقات النقدية المستقبلية "الداخلة والخارجة" من ثم يطرح منها تعديلات المخاطر غير المالية للتوصل إلى هامش الخدمة التعاقدية والذي يمثّل الربح غير المكتسب من مجموعة عقود التأمين.

٣) منهج التكلفة المتغيرة (Variable Fees Approach)

هو المنهج الذي يتم من خلاله تعديل بعض متطلبات المنهج العام لمعالجة عقود الاستثمار التي تتضمن ميزة المشاركة.

- على الشركة إعداد سياسة لقياس ومعالجة عقود التأمين وعقود إعادة التأمين المحتفظ بها معتمدة من قبل مجلس الإدارة يتم تقييمها من قبل الخبير الإكتواري المعين من الشركة، تتضمن بحد أدنى ما يلي:
  - عقود التأمين التي سيتم معالجتها وفقاً لمتطلبات منهج تخصيص الأقساط و/أو المنهج العام و/أو منهج التكلفة المتغيرة.
  - آلية اختبار إمكانية تطبيق منهج تخصيص الأقساط وفقاً لمستوى الأهمية النسبية في الحالات التي تكون فيها فترة التغطية أكثر من عام واحد.
  - آلية تحديد مستوى الأهمية النسبية المستخدمة في اختبار تطبيق منهج تخصيص الاقساط.

عاشراً: الإفصاحات

على الشركة أن تُفصح في بياناتها المالية إضافةً إلى ما ورد في الفقرات من (٩٣) إلى (١٣٢) من المعيار، بالحد الأدنى الجوانب التالية:

- التسويات بين الرصيد الافتتاحي والرصيد الختامي الخاصة ببند الالتزامات مقابل التغطية المتبقية، وبشكل يبيّن القيمة الحالية للتدفقات النقدية المستقبلية، تعديلات المخاطر، هامش الخدمة التعاقدية، مصروف/ ايراد التمويل لكل محفظة على حدا. إضافةً على أن يتم توضيح مكون الخسارة وذلك في حال وجود عقود مثقلة بالأعباء ضمن مجموعات عقود التأمين.
- التسويات بين الرصيد الافتتاحي والرصيد الختامي الخاصة ببند الالتزامات مقابل المطالبات المتكبدة وبشكل يبيّن القيمة الحالية للتدفقات النقدية المستقبلية، تعديلات المخاطر، مصروف التمويل، لكل محفظة.
- معدلات الخصم المستخدمة في احتساب القيمة الحالية للتدفقات النقدية المستقبلية والطريقة المستخدمة والعوامل التي تم الاعتماد عليها في احتساب تلك المعدلات، ومبررات اعتمادها.
- فيما يخص أثر الانتقال إلى تطبيق المعيار، بالنسبة للعقود التي يتم قياسها بموجب النهج الرجعي المعدل أو نهج القيمة العادلة عند التحول إلى المعيار الدولي للتقارير المالية ١٧، يجب الإفصاح عن تسوية هامش الخدمة التعاقدية ومبالغ إيرادات التأمين بشكل منفصل للعقود بموجب كل نهج، بالإضافة إلى مبررات استخدام تلك المناهج.
- العقود التي تصدرها الشركة ولا تنطبق عليها متطلبات المعيار.
- تقديرات الادارة فيما يخص الفرضيات المستخدمة في الجوانب التالية:
  - تقدير التدفقات النقدية.
  - مستوى التجميع.
  - اختبار تطبيق منهج تخصيص الأقساط على العقود التي تزيد فترة تغطيتها عن سنة.
  - تعديلات المخاطر غير المالية.
  - آلية معالجة تكاليف الاستحواذ.
  - فصل عقود التأمين.
  - طريقة معالجة مصروف/ ايراد التمويل.
  - المناهج المحاسبية المستخدمة لكل محفظة على حدا.
  - أي تغييرات في الفرضيات المستخدمة للبنود الواردة أعلاه.

الفصل الثاني
إدارة عمليات أنظمة تقنية المعلومات

أولاً: إدارة مشروع أنظمة تقنية المعلومات الخاص بتطبيق متطلبات المعيار

- حتى تتمكن الشركة من إدارة المشروع بشكل أكثر كفاءة وفعالية على الشركة وضع خطة عمل معتمدة من قبل مجلس الإدارة تتناسب مع طبيعة أعمال الشركة وتعقيد متطلبات المعيار، بحيث تشمل توزيع مهام ومسؤوليات الإشراف والرقابة على مراحل تنفيذ المشروع وعملية إعداد التقارير اللازمة وتقييم المخاطر طوال فترة المشروع.
- عند إعداد خطة العمل المشار إليها أعلاه على الشركة وبالحد الأدنى مراعاة الجوانب التالية:

١) مدى كفاية وكفاءة الموارد المتاحة (خبرات، سيولة، موارد بشرية ...إلخ) بما في ذلك موارد مزود نظام تقنية المعلومات لتنفيذ المشروع بفعالية.
٢) التنسيق بين مختلف دوائر الشركة المرتبطة بتطبيق متطلبات المعيار.
٣) دراسة الجوانب الواجب توافرها في نظام تقنية المعلومات والمتعلقة بمتطلبات المعيار بما يتناسب مع طبيعة أعمال الشركة
٤) مدى كفاية الضوابط الرقابية والأمنية المستخدمة في نظام تقنية المعلومات للتخفيف من مخاطر الأمن السيبراني أو اختراق البيانات.
٥) تحديد التقارير الإدارية التي تحتاجها الشركة لتقييم أدائها، إضافة الى تحديد دورية استخراج تلك التقارير.
٦) إمكانية استرداد البيانات الموجودة لدى مزودي أنظمة تقنية المعلومات في الوقت المناسب.
٧) الاحتفاظ بالنُسخ الاحتياطية في موقع آمن ويمكن الوصول اليه عند الحاجة، وآلية فحصها.
٨) الإجراءات المناسبة للتعافي من الكوارث واختبارها بشكل دوري.

ثانياً: أنظمة تقنية المعلومات

- عند اعتماد مزود نظام تقنية المعلومات من قبل مجلس الإدارة، على الشركة التأكد من قدرة النظام على معالجة الجوانب المبينة أدناه بالحد الأدنى:
  - تخزين البيانات على مستوى العقد وأرشفتها.
  - تجميع العقود وفق المستويات المطلوبة - والمشار إليها في الفصل الرابع -، إضافةً إلى فصل المكونات غير التأمينية عن عقد التأمين.
  - القدرة على تطبيق كافة متطلبات منهج القياس المحاسبي المستخدم والملائم لطبيعة أعمال الشركة.
  - تقدير التدفقات النقدية المستقبلية لتقييم التزامات عقود التأمين بشكل آلي، بحيث تكون الفرضيات الاكتوارية الخاصة بتقديرات التدفقات النقدية مثبته على النظام.
  - احتساب القيمة الحالية للتدفقات النقدية المستقبلية وفق سياسة معدل الخصم المعتمدة من قبل مجلس الإدارة.
  - احتساب قيمة تعديلات المخاطر غير المالية وهامش الخدمة التعاقدية وفق الفرضيات الاكتوارية.
  - إدارة عمليات عقود اعادة التأمين المحتفظ بها بشكل منفصل.
  - إعداد التقارير المالية والإفصاحات المتعلقة بها، إضافة الى التقارير الإدارية.
  - معالجة التغييرات في الفرضيات الاكتوارية المستخدمة في مرحلة القياس اللاحق لمجموعات عقود التأمين.

- قائمة بأسماء وأرقام الحسابات المدرجة ضمن دفتر الاستاذ وفق متطلبات المعيار.
- لائحة بالقيود المحاسبية التقنية لكل منهج معتمد لقياس إلتزامات عقود التأمين)وموجودات عقود إعادة التأمين، بالإضافة الى كافة القيود المحاسبية المتعلقة بإيرادات ومصاريف عقود التأمين وفق متطلبات المعيار المذكور.

- مع مراعاة ما ورد في التشريعات النافذة ذات العلاقة، على مجلس إدارة الشركة الأخذ بعين الاعتبار الجوانب التالية فيما يتعلق بعمليات تدقيق أنظمة تقنية المعلومات:

- التأكد من أن موظفي التدقيق الداخلي لديها على دراية كافية بالممارسات الفضلى لتدقيق أنظمة تقنية المعلومات، والمتطلبات اللازمة لتطبيق متطلبات المعيار.
- تزويد البنك المركزي بتقرير تدقيق أنظمة تقنية المعلومات معد من قبل دائرة التدقيق الداخلي، بكامل المستندات المتعلقة به والتحقق من كفاية أنظمة الضبط والرقابة الداخلية المعتمدة، وأن يبين التقرير نطاق ومنهجية التدقيق وملخص النتائج والإجراءات التصحيحية بشكل سنوي.

الفصل الثالث
قواعد مشاركة وتخزين المعلومات مع طرف ثالث

أولا: الحد الأدنى من القواعد الواجب الالتزام بها عند مشاركة وتخزين المعلومات مع طرف ثالث:

	الجوانب التعاقدية والقانونية
1	على الشـــركة اســـتخدام منهج تقييم قائم على المخاطر لتحديد البيانات المســـموح بتخزينها أو معالجتها خارج الشـــركة وفقًا لطبيعة وتصـــنيف ودرجة مخاطر البيانات مع مراعاة الالتزام بالتشريعات النافذة ذات العلاقة.
2	يجب أن يكون مزود خدمة أنظمة تقنية المعلومات أو/ و الطرف الثالث معروفاً وحسن السمعة، وأن لا يكون لديه ممارسات غير سليمة مع الجهات التي يعمل أو قد عَمِل معها.
3	ابرام الاتفاقيات الخاصـــة بكلٍ من Service Level Agreement و Non-Disclosure Agreement مع مزود خدمة أنظمة تقنية المعلومات أو/ و الطرف الثالث، على أن تحدد الاتفاقيات المعايير التي يتم بموجبها تنفيذ العمليات من قبل مزود خدمة أنظمة تقنية المعلومات أو/ و الطرف الثالث، وأن تتضـمن الشـروط الجزائية والغرامات لأي إجراء أو تصـرّف ينتهك خصوصية وأمن المعلومات.
4	المحافظة على ســرية المعلومات بحيث تتضــمن الامتثال لأحكام ســرية المعلومات وفق قانون تنظيم اعمال التأمين رقم (١٢) لسنة ٢٠٢١، والتشريعات ذات العلاقة.
5	التأكد من أن مزود خدمة أنظمة تقنية المعلومات أو/ و الطرف الثالث يعتمد ضوابط رقابية كافية لتمكينه من الوفاء بالتزاماته التعاقدية والقانونية، مثل الحفاظ على خصـــوصـــية البيانات وإعداد تقارير الامتثال للضوابط الأمنية والرقابية.
6	يجب وضـع إجراءات الاستجابة للحوادث، لضـمان التعامل الفعّال في الوقت المناسـب مع جميع الحوادث التي قد تتعرض لها البيانات.
7	يمكن للشركة أن تستخدم خدمة الحوسبة السحابية من مزود الخدمة مباشرة أو من خلال وسيط، وفي حالة التعامل مع الوسـيط، على الشـركة مراعاة تطبيق كافة المتطلبات والضـوابط الرقابية والأمنية المطبقة على مزود الخدمة.
8	على الشركة تقييم مدى كفاءة وفعالية خدمة الحوسبة السحابية ومدى انسجامها مع متطلبات أمن المعلومات.
9	التأكد من متطلبات خصـوصـية المعلومات عند انتهاء أو فسـخ العقد مع مزود الخدمة أو الوسـيط أو نقلها لمزود خدمة آخر، ويجب حذف كافة البيانات بما فيها النسـخ الاحتياطية من البيانات بعد تسليمها إلى الشركة.

إدارة الوصول إلى البيانات	
1	يجب استخدام اليات التحقق من الهوية والوصول المنطقي (Logical Access) للوصول الى البيانات المخزنة لدى مزود خدمة أنظمة تقنية المعلومات أو/ و الطرف الثالث، حيث يُحظر منح صلاحيات الوصول بشكل واسع والتي تؤدي الى إمكانية وصول أي جهاز/مستخدم غير مصرح به الى البيانات .
2	انشاء قناة اتصال آمنة ومشفرة من خلال -Virtual Private Network -VPN، خاصةً عندما يكون الاتصال Site-to-Site.
3	عدم استخدام بعض البروتوكولات الحساسة مثل (SSH,RDP) من خلال شبكة الانترنت دون وجود ضوابط رقابية كافية ومناسبة، الأمر الذي يؤدي الى استخدامها بطرق غير مصرح بها للوصول الى البيانات.
حماية البيانات	
1	تأكد من أن البيانات المخزنة لدى مزود خدمة أنظمة تقنية المعلومات أو/ والطرف الثالث تُحفظ بمعزل عن بيانات المشاركين الآخرين من خلال اليات العزل اللازمة مثل: Multi-Tenant Environments
2	على الشركة تشفير البيانات أثناء عملية نقل البيانات خلال الشبكة وعند تخزينها على الخوادم و/او وحدات التخزين والنسخ الاحتياطية مع مراعاة استخدام خوارزميات وبروتوكولات تشفير آمنة ومقبولة.
3	وضع الضوابط الرقابية المناسبة على مفاتيح التشفير، وفي حال منح مزود خدمة أنظمة تقنية المعلومات أو/ والطرف الثالث صلاحية الوصول إلى مفاتيح التشفير فإن مسؤولية البيانات تكون على الشركة.
4	التأكد من الأنظمة/ الخدمات لدى مزود خدمة أنظمة تقنية المعلومات أو/ و الطرف الثالث ليست معرضة لأي من التهديدات العشرة المتعلقة بالـ OWASP.
5	حماية جميع الأنظمة عن طريق Anti-Virus/ Anti-malware software و Intrusion Prevention System لمنع أي تدخل أو نشاط يلحق ضرر في البيانات.
6	استخدام Web Application Firewall للتقليل أو ايقاف الهجمات على تطبيقات الويب ونقاط الضعف الموجودة فيها.
7	التأكد من تعزيز ضوابط أمن وحماية البيانات (System Hardening) لجميع التطبيقات والأنظمة والأجهزة وفقًا للممارسات الفضلى.

الحماية المادية	
1	على الشـــركة ومزود خدمة أنظمة تقنية المعلومات أو/ و الطرف الثالث الاحتفاظ بالخوادم والأجهزة المتعلقة بالبنية التحتية لأنظمة تقنية المعلومات بمكان آمن.
2	ضمان الحماية من التهديدات الخارجية.
3	التأكد من ضمان توفير النسخ الاحتياطي وخطة استمرارية العمل لإدامة اعمال الشركة.
4	التأكد من وجود خطة تعافي من الكوارث تتضمن جميع سيناريوهات الكوارث المحتملة، وأن يتم اختبرها بشكل دوري.
حماية عناصر التحقق من الهوية والمصادقة (Credentials)	
1	استخدام طريقة المصادقة الثنائية (Two-Factor Authentication) لكافة الحسابات لتعزيز الحماية عند استخدام اسم المستخدم وكلمة المرور..
2	يُحظر استخدام الحسابات ذات الصلاحيات المطلقة (Built-In Administrator) حيث يجب حفظها في مكان آمن واســتخدامها لبعض الاعمال التي تتطلب ذلك فقط وفي حالات الطوارئ. والاستعاضة عنها بحسابات مخصصة بصلاحيات تقضي حاجة العمل (Least Privileges)
3	يُحظر استخدام Shared Accounts، حيث يجب أن يتم إنشـاء أسـماء المسـتخدمين وكلمات المرور الخاصة حسب مبدأ Least Privilege، والفصل بين المهام والصلاحيات.
4	تطبيق الممارسات الفضلى في سياسة ومعايير كلمات المرور وإدارة الجلسات.
5	حماية كلمات المرور والمفاتيح الأمنية الخاصة بـ Application Programming Interface وتغييرها بشكل دوري.
السجلات الأمنية والتدقيق	
1	التأكد من تفعيل سـجلات الاحداث الأمنية والتنبيهات بحيث تشـمل الحسـابات التي يتم انشـاءها، وصـــف الحدث والتاريخ والوقت وغيرها من الأمور ، على أن يتم مراجعة الســجلات لمراقبة واكتشاف الحركات المشبوهة وتحديد النشاطات غير الطبيعية.
2	على مزود خدمة أنظمة تقنية المعلومات أو/ و الطرف الثالث تنبيه وإخطار الشــركة في حالة طلب الوصول إلى البيانات من قبل أي جهات أخرى.
3	الوصـول في الوقت المناسـب إلى السـجلات اللازمة للتدقيق والتحقيقات الجنائية، والإبلاغ عن المعلومات ذات الصلة بالبيانات أو التطبيقات المحددة للشركة.

ثانياً: الحد الأدنى من القواعد الإرشادية التي يُنصح تبنيها:

الجوانب التعاقدية والقانونية	
1	على الشـــركة أو مزود خدمة أنظمة تقنية المعلومات أو/ و الطرف الثالث القيام بإجراء Penetration Testing and Vulnerability Assessment بشكل دوري، وفي حال قيام مزود الخدمة بإجراء تلك الاختبارات يجب أن يتم تقديم تقرير بالنتائج للشركة.
2	إجراء Scenario-Based Risk Assessment and Planning Activity بشكل دوري من أجل: - تحديد الطرق التي من الممكن أن تسمح بالوصول إلى البيانات بشكل غير مصرح به. - تحليل فعالية ضوابط المنع والكشف الحالية للتخفيف من احتمالية الوصول غير مصرح به للبيانات. - تحليل احتمالية وتأثير Significant and Plausible Attack Vectors في ضوء الضوابط الرقابية المستخدمة. - تحليل فعالية ضوابط الاستجابة المستخدمة للحد من تأثير Significant and Plausible Attack Vectors. - تحديد الحاجة إلى ضوابط وقائية أو كشفية إضافية.
3	توافر المؤهلات والخبرات الملائمة لدى مزود خدمة أنظمة تقنية المعلومات أو/ و الطرف الثالث والفريق المسؤول عن إدارة بيانات الشركة للتأكد من أداء مهامهم بكفاءة وفعالية.
إدارة الوصول إلى البيانات	
1	يجب وضع الضوابط الرقابية الملائمة وبشكل مقيد لإدارة عملية الوصول إلى البيانات (Restricted Access) من خلال الشبكة (i.e. Restrict public IP)، وعدم تفعيل صلاحيات الوصول العامة (Global Access).
2	استخدام Mutual Authentication أو المصادقة الثنائية للسماح بالوصول البيانات المخزنة.
حماية البيانات	
1	مراعاة ان تكون عملية التشفير تتبع مبدأ (Fail-Safe) بحيث ان تعطل الية/ادوات التشفير او حدوث خلل في الضوابط الأمنية لا تؤثر على البيانات المشفرة، وفي حال تمكنت أطراف خارجية غير مصرح لها من الوصول إلى البيانات أن تكون غير قابلة للقراءة ولا يمكن الاستفادة منها.
2	تقييم متطلبات أمن المعلومات المطبقة لدى مزود خدمة أنظمة تقنية المعلومات أو/ و الطرف الثالث، من خلال التأكد من الامتثال لمعايير أمن البيانات وتنفيذ penetration testing, vulnerability scanning وتقييم المخاطر بشكل مستمر.

حماية عناصر التحقق من الهوية والمصادقة (Credentials)	
1	اعتماد آلية لمراجعة حسابات المستخدمين والصلاحيات بشكل مستمر وإلغاء او تعطيل الحسابات غير المستخدمة.
2	يجب مراعاة التسمية الموحدة (Naming convention) لجميع الحسابات والأصول، وان لا يشير اسم الحساب للصلاحيات الممنوحة.
السجلات الأمنية والتدقيق	
1	يجب استخدام التقنيات التي تراقب وتفحص باستمرار الإعدادات الأمنية المطبقة بشكل دوري.
2	يجب استخدام الممارسات الفضلى المتعلقة بـ Application Programming Interface في مجال الاختبار والتدقيق وحماية الأنشطة غير الطبيعية.

ثالثا: أهم المعايير الواجب استخدامها في مجال تكنولوجيا الحوسبة السحابية

الموضوع	المعايير
الحوكمة وإدارة المخاطر والامتثال	• COBIT • ISO/IEC 20000 • SSAE 16 or ITIL depending on type of workload • ISO/IEC 27001 and ISO/IEC 27002 • ISO/IEC 27017 & ISO/IEC 27018 • ISO/IEC 38500 – IT Governance • Cloud Security Alliance (CSA) Cloud Controls Matrix • National Institute of Standards and Technology (NIST) • Cybersecurity Framework (CSF)
العمليات التشغيلية و التجارية	• SSAE 16 • ISO/IEC 27000
إدارة الأدوار	• LDAP, SAML 2.0, OAuth 2.0, WS-Federation, OpenID Connect, SCIM • XACML • PKCS, X.509, OpenPG
حماية البيانات و المعلومات	• HTTPS, SFTP, VPN using IPSec or SSL • OASIS KMIP • US FIPS 140-2
سياسات الخصوصية	• ISO/IEC 27018
أمن وحماية الشبكات	• ISO/IEC 27033 or FIPS199/200 standards
الضوابط الأمنية على البنية التحتية	• ISO/IEC 27002 • ISO/IEC 27017 & ISO/IEC 27018
شروط الأمان في اتفاقية مستوى الخدمة	• ISO/IEC 19086 • ISO/IEC 27004:2009, TM Forum TR 178, NIST Special Publication 800-55, CIS Consensus Security Metrics V1.1.0, and ENISA Procure Secure • CWE list • CSA STAR registry • PCI DSS • FedRAMP program

الفصل الرابع
العمليات الإدارية

أولاً: التخطيط والموازنات التقديرية

- على الشركة تحديد الأسس والفرضيات الخاصة بإعداد الموازنات التقديرية بشكل بتناسب مع متطلبات المعيار لضمان توافق التقارير الإدارية مع التقارير المالية.

ثانياً: العمليات الإكتوارية

- تتكون العمليات الإكتوارية المتعلقة بمتطلبات المعيار مما يلي:
  - تسعير عقود التأمين.
  - تحديد مدى كفاية قيمة التزامات عقود التأمين.
  - وضع فرضيات لعملية تقدير التدفقات النقدية المستقبلية.
  - تقييم ربحية العقد
  - تحديد معدلات الخصم.
  - تحديد هامش الخدمة التعاقدية عند الاعتراف الاولي والقياس اللاحق.
  - تحديد تعديلات المخاطر غير المالية عند الاعتراف الأولي والقياس اللاحق، وأسلوب التقدير المناسب.
  - مستوى التجميع.
  - المشاركة في تحديد مؤشرات الأداء الرئيسية.
  - تحليل الحساسية.

ثالثاً: عمليات إدارة المخاطر

- يجب أن يتوفر لدى الشركة بحد أدنى ما يلي:
  ١) لجنة إدارة المخاطر.
  ٢) ميثاق إدارة المخاطر.
  ٣) سياسة إدارة المخاطر.
  ٤) المستوى المقبول من المخاطر.
  ٥) إطار مراقبة المخاطر والتقييم الذاتي للمخاطر.
  ٦) سياسة إدارة مقابلة الموجودات والمطلوبات.

- يجب أن تقوم الشركة بتحديد وقياس المخاطر الناتجة عن التغيير في السياسات المحاسبية والإكتوارية وغيرها من الجوانب المتعلقة بمتطلبات المعيار، بحيث يتم تحديد المخاطر لكل دائرة من دوائر الشركة ذات العلاقة.
- يجب على الشركة مراعاة عدم وجود حالات تضارب مصالح عند التعاقد مع أية جهة لتقديم خدمات مرتبطة بتطبيق متطلبات المعيار سواء كانت خدمات مرتبطة بأنظمة تقنية المعلومات أو خدمات استشارية لإدارة مشروع تطبيق متطلبات المعيار وذلك بالتزامن مع خدمات تدقيق حسابات الشركة أو خدمات دراسة مدى كفاية المخصصات الفنية المطلوبة حسب التعليمات النافذة.